
The Association Executive's Guide to Protecting Real Estate Information



Version 1.0
November 2004

Contents

1. Executive Summary	4
2. Protecting Member and Consumer Trust	7
3. Business Principles	7
4. Information Security Guidelines	8
5. Information Ownership	9
6. Managing Information Security	10
7. Acceptable Use	12
8. Authenticating Identity	13
9. Disclosing the “Standard of Care”	14
10. Labeling Sensitive Information	15
11. Keeping Personal Information Private	16
12. Involving Your Trading Partners	17
13. Securing Sensitive Information	18
14. Technology	19

15. Responding to an Event:	20
16. Education and Training	21
17. A Community Responsibility	21

The Association Executive's Guide

to Protecting Real Estate Information

1. Executive Summary

Protecting and controlling real estate information has become critical to the business success of members and the operations of associations. Realtors® and their associations should embrace best practices for information security to respond to several changing market forces, including the following:

Protecting and controlling real estate information has become critical to the business success of members and the operations of associations.

Customer Trust	Consumers have a number of choices to assist them with their real estate needs. Realtors® need to improve their information security practices to enhance their traditional position as the first point of consumer contact, and facilitator of the real estate transaction.
Privacy	Identity theft, fraud, unwanted solicitations, malicious viruses, and other highly publicized threats have increased awareness of the need to better protect the privacy of personal information. Associations need to improve their protection of member information and help members understand the need to improve their information security practices to meet and exceed consumer expectations that their personal information will be protected.
Regulation	Associations and their members 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 consumer and transaction information place members at risk. Associations need to improve their information security practices to mitigate the liability resulting from any compromise of consumer, member, and business partner information.
Piracy	Information about member is of tremendous commercial value to marketers and may be subject to unauthorized access and uses. Associations need to improve information security practices to create a chain of custody that can control how member information is used.
	Members assume liability, add creative expression

Rights	and frequently compile listing and other forms of information. Associations and Realtors® should assert their ownership through copyright and technology protections of their intellectual property.
Efficiency	The workflow of a real estate transaction is complex and involves many participants. Many organizations are pursuing initiatives with the ultimate goal of reducing the costs, complexity and risks associated with the transaction process. Associations need to assist members in developing, integrating and managing new standards for the secure exchange of real estate information.
Costs	The real estate industry can improve information security through the use of new technologies. Associations and members should use proven commercial technologies in order to lower the cost of implementing information security.

These guidelines will help associations to assess their information security readiness, better secure member information, reduce costs, and improve the effectiveness of their member’s business operations. Associations should work to support legislation and regulation that serves the information needs of members and prevents third parties from acquiring member information for commercial purposes.

A breach in consumer trust can result in significant damage to our industry’s reputation and professional image.

A breach in consumer trust can result in significant damage to our industry’s reputation and professional image. Associations should integrate information security into their governance programs and create policies to reduce the risk of compromising the confidentiality, availability and integrity of member information.

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

Association Executives	
Essential Information Security Programs and Practices	
1	Educate members on NAR information protection principles and information security guidelines
2	Appoint an information security committee to define member information security policies and practices and implement programs for secure information exchange.
3	Design digital trust programs for the implementation of guidelines and approved changes to the guidelines.

A breach in consumer trust can result in significant damage to our industry's reputation and professional image.

4	Publish "standards of care" and "business continuity plans" that may be applied to member and consumer personal information, and trading partner business information
5	Define consumer and trading partner disclosures based on accepted standards of care.
6	Define confidentiality and intellectual property agreements that specify broker rights to all information, pictures and other intellectual property created by agents and others while in the employ of a brokerage or MLS.
7	Establish training programs for members and staff on how to use, administer, and maintain sensitive information and systems.
8	Engage external organizations that can conduct a periodic review of information controls to determine compliance with the association security policies and practices.
9	Define the process for assuring the identity of an individual and systems based on the sensitivity of the information that they will have access to.
10	Engage regulators, commissions and other public policy bodies as required on industry information security issues.

These, and the additional guidelines included in this document, will help associations control the activities of third parties who attempt to acquire member information for unauthorized commercial purposes.

2. Protecting Member and Consumer Trust

Trust is based upon the expectation of fair and honest dealings. Consumers trust members to manage their largest single purchase and most important financial investment. Consumers also trust members with information about their properties, financial qualifications and purchasing intentions. Likewise, members must trust associations with their information.

Protecting member information has become far more difficult because digital information can be so easily copied, stolen, repackaged, destroyed or maliciously altered. The pervasive use of the Internet makes it possible for digital information to be transferred to many organizations without a member's knowledge. Association need new management tools and technologies to better control the flow of their information and protect the information they and their members create exchange and publish.

Our customers are increasingly aware of the importance of protecting their personal information.

Expectations are changing. Members and customers are increasingly aware of the importance of protecting their personal information. They understand that the careless handling of information can harm individuals and businesses. Furthermore, new and proposed government regulations impose penalties on organizations that fail to secure or improperly use the personal information in their care. Associations are accountable to members, consumers, trading partners and, increasingly, regulators for the protection of personal and business information. Associations should reduce these growing risks of liability and business disruption from ever-changing internal and external threats.

Associations and their members incur the cost of capturing and creating information and assume regulatory liability for the performance of their businesses. Associations should lead in the effort to manage the shared risks, and improve the information security and controls of, a highly interconnected and information intensive industry.

3. Business Principles

The National Association of Realtors® has defined a set of principles to assist members as they improve their information protection policies, practices and protections. These principles help assure users, partners

and third parties that Realtors® will exercise care in the creation, maintenance and distribution of all forms of Realtor® information. The principles are as follows:

Business Principles

Customer Trust	Customer trust is critical to Realtors® success. Realtors® should inform customers about 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.
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.

Local and state associations have a vital role in educating their members on the importance of protecting Realtor® information.

Local and state associations have a vital role in educating their members on the importance of protecting member information and designing effective governance policies and programs to improve information security.

4. Information Security Guidelines

The National Association of Realtors® has developed a comprehensive set of guidelines, based upon accepted standards and best practices, to help its members mitigate information security risks. The guidelines for agents, brokers, associations and Multiple Listing Services (MLSs) are intended to educate and assist NAR members in improving their operations, specifically to:

Community Responsibilities
Fulfill contract obligations by ensuring that information providers and users of member information are aware of their responsibilities.
Assert ownership of information by ensuring that the owners and custodians of information take active measures to protect member rights.
Ensure compliance with regulatory requirements by placing the responsibility and accountability for compliance upon owners of information.
Prevent misuse of information and avoid liability by creating, adopting, and complying with a standard set of guidelines that mitigate a common set of risks.
Create a vigilant environment that attempts to proactively identify existing and emerging risks to member information.
Avoid disruption and plan for business continuity by ensuring procedures are in place to maintain reasonable availability of information systems.
Establish the basis for integration of security conventions by creating commonly understood approaches based on commercial off- the- shelf technology.
Ensure the participation of members in the full range of transaction services that are dependent on best information security practices, procedures and technologies.

These guidelines are influenced by the ISO 17799 format that is the international standard for information security best practices. They highlight the factors most relevant to the operations of each member constituency. Associations should understand importance of implementing these guidelines and consider enhancing their information protection education and governance programs.

5. Information Ownership

The ability of members to operate in a secure manner that preserves their rights to information and serves consumer privacy interests is fundamental to retaining the member's competitive advantage.

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

Real estate information has commercial value to many inside and outside the real estate industry. Brokers should assert their ownership

to the information they create and control the information “chain of custody” that extends from the agent to third party information aggregators such as MLSs, portals and commercial and government information providers. Associations should educate members to take several actions to assert their ownership to their information.

Ownership Best Practices	Assessment
Enter into confidentiality and intellectual property agreements that specify broker rights to 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 association, brokerage or MLS. Identify information to which the organization adds creative expression (e.g. remarks and descriptions created by an agent).	
Consider copyright protections for the information created, captured, compiled and published by a brokerage or Multiple Listing Service (MLS).	

Associations should identify the information “Owners” of all information under its control. The Owner should ensure that ownership rights have been clearly identified, and specify the security classification, access rights and retention policies for association information.

Multiple Listing Services should be designated as “custodians” of broker provider information and as “owners” of information resources (databases and other repositories) that they create and compile. In all cases broker rights should be specified when broker information is used by an MLS to create new information resources.

6. Managing Information Security

Associations should appoint an Information Security Committee to lead the development and maintenance of internal and member information security policies. The committee should be comprised of senior managers from member organizations and selected staff. This committee should be responsible for the following:

Governance Best Practices	Assessment
Meet on a regular basis to review and educate their members on the information security	

guidelines.	
Review any proposed changes to the guidelines and make appropriate recommendations for final approval.	
Design programs for the implementation of approved changes to the guidelines.	
Manage the training and dissemination of newly incorporated changes to the guidelines.	
Direct compliance, audit and sanctions activities.	
Coordinate security related activities among member organization entities and information owners.	
Represent members in industry information security activities.	

Responsibility for information security on a daily basis rests with every member and association employee. Associations should identify a “security manager” to oversee the physical and information security needs of the organization. The security manager should coordinate the association’s efforts to prevent loss or compromise of the organization’s business critical and sensitive information. The association security manager’s responsibilities should also include:

Security Manager Best Practices	Assessment
Performing information security risk assessments.	
Preparing information security management action plans.	
Developing information security correction plans.	
Communicating incident alerts through appropriate channels.	
Participating in the development of business continuity plans.	
Investigating information security breaches.	
Participating in information security training and awareness programs.	

All consultants, contractors, and others performing duties on behalf of associations should be subject to the same information security responsibilities as association employees.

Association executives and/or the designated security manager should also create, maintain and periodically reconcile an inventory of information resources including all hardware, software and data files. All microcomputer equipment should be marked with visible identification that clearly indicates that it is association property.

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

Improperly installed or configured wireless access points are a major security risk, potentially exposing the entirety of the Association'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. Users and employees should be instructed never to install a wireless access point in the Association offices without the authorization and assistance of the Association security manager.

All users 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).

7. Acceptable Use

Information should be treated and managed as a valuable business resource. Associations provide information and access to information systems to employees, contractors, business partners, suppliers and members. Associations 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, associations should 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 connect any device to the organization's network without express prior approval from the Security Manager and the organization's IT department.	
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.	

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

Associations should include language supporting the Acceptable Use Guidelines in applicable contractor, supplier and other third party business agreements.

8. Authenticating Identity

Establishing identity is the first step to effectively managing access to information and information systems. Associations should define the process for establishing the identity of an individual or member based on the sensitivity of the information to which they will have access. This process may involve inspection of government documents, establishing a password or PIN based on shared secrets or simply a destination (address or email). Associations should take extra care in safeguarding information about identity and the credentials that are used to access information and systems.

Association employees and members should be instructed to never download any files or open any email attachments they are not expecting. These files may contain a virus or include other forms of malicious software that can damage the association’s systems. Consider verifying the phone number and email address of individuals who register at a Website before exchanging listings or other information.

Associations 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 association assets the prospective employee or contractor will have access to.

9. Disclosing the “Standard of Care”

An association should disclose the “standard of care” it will apply to protecting a member’s personal information. Associations should employ the following disclosure practices:

Disclosure Best Practices	Assessment
Association should not collect or store any information not directly related to an approved association business purpose.	
Associations should disclose to members when their information may be used for statistical analysis.	
Associations should offer members reasonable access to the information they have collected about them, including a reasonable opportunity to review information and to correct inaccuracies and delete information.	
Associations should take active measures to protect member information from unauthorized access, alteration, destruction, modification or disclosure.	
Associations should ensure that sensitive information is protected in transit over the Internet and that physical and technical safeguards are in place to provide authorized access to personal information.	
Associations should authenticate individuals who have access to personal information to a level of assurance commensurate with the	

sensitivity of the information.	
Associations should alert members that they can be held accountable for the proper handling of consumer information.	
Associations should disclose a breach of information security to members whose information may have been disclosed to unauthorized persons.	

These disclosures should be published on the association’s websites and include links to the Realtor® Code of Ethics.

10. Labeling Sensitive Information

Some forms of association information are especially sensitive and should always be labeled as confidential and, in some cases, secret. Associations who operate MLSs recognize that 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.

Member profiles that may describe purchasing histories, interests or other attributes should also be categorized and labeled as confidential. This information is very valuable to third parties and may be subject to theft. Social security numbers, financial qualifications, business performance records, credit card numbers, company profiles, communications histories, member dues or other transactions should always be labeled as secret and subject to the highest level of protection.

Associations also maintain sensitive business records, market research, legislative strategies, employee compensation and evaluations, sales results and forecasts. Member non-public contact information, directories, email addresses and access numbers are highly sensitive. This information should always be categorized and labeled as secret. If sensitive information is lost or is suspected of being disclosed to unauthorized parties, the information Owner and the manager of any affected member organization should be notified immediately.

11. Keeping Personal Information Private

Associations should ensure that the personal information of members, employees and contractors in the association's possession is never disclosed without their written consent.

Some forms of member information are subject to specific federal and state regulation. Associations capture member names, telephone numbers, addresses and email addresses, and should take care to ensure they are not inadvertently disclosed. In some cases, associations may also create electronic files that include social security number and/or driver license and credit card information. Associations should take specific active measures and employ technical solutions, such as encryption, to ensure that this personally identifiable consumer information remains private.

Associations should have a member specified 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 an association'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 association information should be securely destroyed when it is no longer needed for business purposes. Association executives should create an information retention plan with legal counsel to determine the appropriate retention periods for the information. Associations should not destroy or dispose of potentially important records or information without specific management approval. Unauthorized destruction or disposal of association records or information should result in disciplinary action.

12. Involving Your Trading Partners

Associations exchange information with a wide variety of trading partners including member companies, governments, other associations, services providers and affinity partners. Any sensitive information shared between business partners should be subject to a confidentiality or nondisclosure agreement (NDA). Associations should ensure that the information exchanged between trading partners is adequately protected. These practices include:

Information Exchange Best Practices	Assessment
Identifying the information the association or its members considers confidential or secret.	
Identifying what sensitive information the association receives from trading partners.	
Understanding the standards of care the trading partners will apply to association information, and disclosing your standard of care to business partners.	
Entering into confidentiality agreements drafted by legal counsel with any organization that has access to association information systems.	
Entering into information licensing agreements, drafted by legal counsel, only after specific authorization from the Information Owner.	
Ensuring that current license agreements exist for all software programs installed on association owned and operated systems.	
Inspecting the security provisions of Internet Services Providers (ISPs) and other third parties and contractors.	
When choosing and deploying RETS Servers, Associations should ensure that their RETS Server vendor is providing RETS access in a manner consistent with local MLS data access policy (i.e. typically using the same roles, permissions and business rules as supported in the MLS system itself). Associations should take care to ensure their RETS Server vendor is not bypassing local MLS data access policy, but rather supporting and implementing policy	

The rights of a trading partner to use or re-purpose association information should be defined at the time the information is created. The rights associated with many forms of association information such as publications should be described on any documents or published materials.

Digital information is highly vulnerable to unauthorized copying, repackaging and theft. It is especially important that associations ensure that they do not violate the copyright protections of third party information they use in their business.

Associations should contractually specify the rights associated with all 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.

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

Associations 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.

13. Securing Sensitive Information

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

Associations are responsible for ensuring that sensitive information under their control is not compromised through unauthorized access, or manipulation. Confidential documents and sensitive information can be compromised and tampered with when transmitting the information, exchanging the information on electronic media or through unauthorized access. 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. Associations should change the user passwords on their systems at least every 90 days and the password should be a minimum of 8 upper and lower case characters. Sharing or publishing a password or authentication token by an employee should be subject to disciplinary action.

Any attempt to tamper with or gain access to an association’s system or information files by an unauthorized individual should be reported immediately to association management, MLS, third party service provider, and in severe cases, law enforcement.

14. Technology

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

Associations should ensure that they use mature security technologies that are available to reduce the risks to information security. Best practices include the following:

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,	
Install monitoring software to audit sensitive transactions,	

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 associations 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 operations for vulnerabilities. These and other active measures will help ensure associations and other Realtor® organizations can avoid disruption and liability, and sustain a high level of member trust.

An independent review of information system controls should be periodically conducted to determine the 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.

15. Responding to an Event

The effective implementation of best information security practices can prevent or reduce serious business losses or disruption. Despite the association’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 a supplied service or utilities. A Business Continuity Plan should help minimize the disruption to association 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 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 business partners should a major event occur. Contact law enforcement in any case where you suspect intentional or malicious damage to business and information resources.

16. 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. Associations should establish a training and education program for staff that use, administer and maintain sensitive information and systems. These programs should:

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 Realtor® system or information resource.	
Update all users on the local, state and national policies that may affect the protection of Realtor® information.	

Associations 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 or association executive for appropriate handling.

17. A Community Responsibility

The Internet created a major shift in the way members collect and publish listing information to consumers. The next major shift will involve how all forms of real estate information are protected and controlled. The need for members 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 associations continue to work to improve the information security procedures and technology protections of their members and of association 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 and MLSs will invest in technologies that provide more efficient transactions. Greater convenience and service quality must also include the preservation of consumer privacy and control of member information.

Association executives have a vital role to play in the evolution of the industry's information security governance, management and technology infrastructure. Members operate in an interconnected industry where the security of all systems can be compromised by the weakest link. The broad adoption of information security guidelines will help members secure and control all their information, continuously adapt their operations and remain the consumer's trusted advisor in an increasingly competitive and complex marketplace.

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