
The MLS Executive's Guide to Protecting Real Estate Information



**Version 1.0
November 2004**

Contents

1. Executive Summary	4
2. Business Principles	7
3. Information Security Guidelines	7
4. Information Ownership	8
5. Managing Information Security	9
6. Acceptable Use	10
7. Authenticating Identity	12
8. Disclosing the Standard of Care	12
9. Labeling Sensitive Information	13
10. Keeping Personal Information Private	14
12. Involving Your Trading Partners	14
13. Securing All Sensitive Information	16
14. Community Outreach	17
15. Securing Systems and Facilities	18
15.1 Change Control Process	18
15.2 Tet Environmnet	18
15.3 Software Protection and Control	21

15.4 Network Management, Controls, and Operations.....	221
15.5 Segregation of Duties	22
15.6 Facility Management Oversight	22
15.7 Procedures Documentation	23
15.8 Records Management and Retention	24
16. Securing End User Applications	24
16.1 E-mail	24
16.2 Desktop Systems	26
16.3 Public Access Sites.....	27
16.4 Wireless Communications	29
17. Responding to an Event	29
18. Education and Training	33
19. A Community Responsibility	33

The MLS Executive'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 agents and brokers to manage their largest single purchase and most important financial investment. Consumers also trust practitioners with information about their properties, financial qualifications, and purchasing intentions. Protecting broker information has become far more difficult because digital information can be so easily copied, stolen, repackaged, destroyed, or maliciously altered or damaged. The pervasive use of the Internet makes it possible for digital information to be transferred to many organizations without the knowledge of the owner of the information. Practitioners need new management tools and technologies to better control the flow of their information and protect the information they create, exchange, and publish.

Realtors® are accountable to consumers, business partners, and, increasingly, regulators for the protection of personal and business information.

Consumer expectations are changing. Customers are increasingly aware of the importance of protecting their personal information. They recognize that the careless handling of health and financial information can harm individuals and businesses. Furthermore, new and proposed government regulations impose penalties on organizations that improperly use or fail to secure the personal information in their care. Realtors® are accountable to consumers, business partners, and, increasingly, regulators for the protection of personal and business information.

Protecting and controlling real estate information has become critical to the business success of real estate practitioners and the operations of an MLS. Agents, brokers, and MLS executives should embrace best practices for information security to respond to several market forces, including the following:

Customer Trust	Consumers have a number of choices to assist them with their real property needs. Real estate practitioners 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 consumer awareness of the need to better protect the privacy of their personal information. Members need to improve their information security practices to

	meet and exceed consumer expectations that their personal information will be protected.
Regulation	Members will increasingly be subject to new information security regulations. Members 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. They need to improve their information security practices to mitigate the liability resulting from any compromise of consumer and business partner information.
Piracy	Member information such as customer lists, property listings, qualifications, and contract terms is of tremendous commercial value and may be subject to unauthorized access and uses. Members need to improve information security practices to create a chain of custody controlling the use of information.
Rights	Real estate practitioners assume liability, add creative expression, and frequently compile listing and other forms of information. They should assert their ownership through copyright and technology protections of their intellectual property.
Standards	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. Members need to develop, integrate, and manage 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. REALTORS® should use proven multipurpose commercial technologies in order to lower the cost of implementing information security across all their operating environments.

Improving information security is a fundamental requirement in today's real estate industry. These guidelines are intended to help an MLS improve its information security operations and oversight and prevent unauthorized third parties from acquiring Realtor® information for commercial purposes. An MLS should implement procedures and technologies to reduce the risks to the confidentiality, availability, and integrity of real property information. These guidelines will also help an MLS comply with existing and proposed regulations, reduce costs, and improve the efficiency of its operations.

An MLS should implement procedures and technologies to reduce the risks to the confidentiality, availability, and integrity of real property information. Of particular importance are the following essential information security practices that MLSs should implement:

MLS Executives Essential Information Security Practices	
1	Appoint an information security manager to lead the development, maintenance, and enforcement of member information security policies.
2	Enforce confidentiality and intellectual property agreements that specify broker ownership, rights, and consideration to their intellectual property.
3	Define and implement standards of care and business continuity plans that the MLS will apply to member, consumer, and trading partner business information.
4	Define and implement a process for assuring the identity of an individual and systems based on the sensitivity of the information that they will access.
5	Take active technology measures, like encryption, data markers, virus and spyware protection, Wired Equivalent Privacy (WEP) in wireless environments, and auditing systems, to protect member information from unauthorized access, alteration, destruction, modification, or disclosure.
6	Establish minimum security standards for member systems and applications that access MLS systems.
7	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.
8	Implement a change control process to ensure that system changes are documented and tracked to ensure the impact on critical business operations is minimized and inadvertent damage is prevented.
9	Enter into information licensing agreements, drafted by legal counsel, only after specific authorization from members and other information owners.
10	Engage external organizations to conduct a periodic review of information controls to determine compliance with the MLS security policies and practices.

MLSs are a critical component of the real estate industry’s infrastructure. MLS executives should lead effort to help brokers manage the shared risks and improve the information security and controls of a highly interconnected and information-rich industry.

2. Business Principles

The National Association of Realtors® has defined a set of principles to assist members in improving their information protection policies and practices. These principles can help assure users, providers, and third parties that agents, brokers, and MLSs will exercise care in the creation, maintenance, and distribution of their information. An MLS should implement both the letter and the spirit of the following principles:

Business Principles

Customer Trust	Customer trust is critical to Realtors® success. Realtors® 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.
Standards	The broad adoption of information and transaction standards will improve 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.

MLS executives have a vital role in educating their members on the importance of protecting content and implementing effective programs, procedures, and technology to improve information security.

3. Information Security Guidelines

The NAR has developed a comprehensive set of guidelines, based upon best practices, to help its members more effectively manage information security risks. The guidelines for agents, brokers, associations, and MLSs are intended to assist 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 member information take active measures to protect their 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
	Identify threats and vulnerabilities by creating 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 MLSs, associations, brokerages, commercial real estate operations, and real estate practitioners. MLS executives should promote the importance of implementing these guidelines to their members.

4. Information Ownership

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

Member content has commercial value to many inside and outside the real estate industry. MLS executives should help create and ensure member control of the content “chain of custody” that extends from the agent to third-party information aggregators, Web site operators, and commercial and government information providers. MLSs should take several actions to help protect broker ownership of their information including the following:

Ownership Best Practices	Assessment
Enter into intellectual property agreements that specify ownership of all information, pictures, and other intellectual property created by agents and others while in the employ of—or affiliated as an independent contractor with—a brokerage or MLS.	
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, compiled, and published by a brokerage or MLS.	

MLS executives should identify the “owner” of all information under their control. The owner should define the security classification, access, and usage rights and retention policies for MLS information.

MLSs should be designated as either “owners” or “custodians” of the information resources (records, files, databases, and images) that they create and compile from multiple information sources. In all cases broker rights should be specified when broker information is used by an MLS to create new information assets.

5. Managing Information Security

MLS executives should participate in Information Security Committees that lead the development and maintenance of information security policies. The committee should be comprised of senior managers from member organizations. This committee should be responsible for the following tasks:

Governance Best Practices	Assessment
Meet on a regular basis to review and educate their members and affiliates on the Information Security Guidelines	
Review any proposed changes to the guidelines and making appropriate recommendations for final approval by MLS leadership	
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 the MLS in industry information security activities	

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

Security Manager Best Practices	Assessment
Perform information security risk assessments	
Prepare information security management action plans	
Develop information security 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 others that perform duties on behalf of an MLS should be subject to the same information security requirements, and have the same information security responsibilities, as MLS employees.

MLS 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 MLS property.

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

6. Acceptable Use

An MLS provides information and access to information systems for use by employees, contractors, business partners, suppliers, and

members. MLS executives should develop and publish acceptable use guidelines to establish the 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 connect any device to the organization's network without express prior approval from the security manager and the organization's IT department	
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.	

As a convenience, the MLS should specify the incidental 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.

MLS executives should include language that supports the acceptable use guidelines in applicable contractor, supplier, and other third-party business agreements.

7. Authenticating Identity

The security of MLS information starts by establishing the identity of individual users.

The security of MLS information starts by establishing the identity (authenticating) of individual users. It is important to establish the identity of an individual before providing access to any MLS information system.

MLS executives 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 information assets to which the prospective employee or contractor will have access.

Establishing identity is the first step to effectively managing access to information and supporting systems. MLS executives should define the process for establishing the identity of an individual 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, or simply creating a destination (address or e-mail). MLS organizations should take extra care in safeguarding information about identity and the credentials used to access information and systems.

Employees and members should be instructed to never download any files or open any unexpected e-mail attachments. These files may contain a virus or include other forms of malicious software that can damage the organization systems. If MLS policies require consumers to register at a Web site, consider verifying the phone number or e-mail address before exchanging listing or other information.

8. Disclosing the Standard of Care

Disclosing the standard of care you will apply to a member's personal information is always a good business practice. MLS organizations should disclose the following to members:

Disclosure Best Practice	Assessment
MLSs should not collect or store any information not directly related to a leadership-approved business purpose.	
MLSs should disclose to members and other	

information providers when their information may be used for statistical analysis.	
MLSs 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.	
MLSs should take active measures to protect member information from unauthorized access, alteration, destruction, or disclosure.	
MLSs should ensure that all confidential or secret information is protected in transit over the Internet and that physical and technical safeguards are in place to provide authorized access to confidential or secret information.	
MLSs should authenticate all individuals who have access to confidential or secret information to a level of assurance commensurate with the sensitivity of the information.	
MLSs should hold brokers, other MLSs, and other affiliates accountable for the proper handling of consumer and Realtor [®] business information.	
MLSs should disclose a breach of information security to members whose information may have been disclosed to unauthorized persons.	

These disclosures should be published on all MLS Web sites and include links to the Realtor[®] Code of Ethics.

9. Labeling Sensitive Information

Some MLS information is especially sensitive and should always be identified and labeled as confidential or, in some cases, secret. Specific remarks, compensation terms, contract 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 all passwords, should always be labeled and handled as secret.

Profiles that specify local market sales results, sales histories, market trends, and company performance or other market attributes should also be categorized and labeled as confidential or secret. This information is very valuable to third parties and may be subject to malicious attack by hackers or others.

MLS organizations also maintain sensitive business records, market research, employee compensation and evaluations. 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 organization should be notified immediately.

10. Keeping Personal Information Private

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

Some forms of member information are subject to specific federal and state regulation. MLS organizations routinely capture member name, telephone number, street address, and e-mail address information and should take care to ensure they are not inadvertently disclosed.

Member, employee, or consumer personal information should not be removed from an MLS'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 MLS information should be destroyed or disposed of when it is no longer needed for business purposes. MLS executives should assess the continued value and usefulness of information on a periodic basis. MLS executives should create a data retention plan with legal counsel to determine the appropriate retention periods for information. MLSs should not destroy or dispose of potentially important records or information without specific management approval. Unauthorized destruction or disposal of the organization's records or information should result in disciplinary action.

12. Involving Your Trading Partners

MLS organizations exchange information with a wide variety of business partners including members, local governments, associations, service providers, and publishers. Any sensitive information shared between business partners should be subject to a confidentiality or nondisclosure agreement. An MLS should ensure that the information exchanged between business partners is adequately protected. These practices include the following:

Information Exchange Best Practice	Assessment
Identify the information that the MLS or its members consider confidential or secret	
Identify what sensitive information the MLS receives from business partners	
Understand the standards of care business partners will apply to MLS information and disclosing the MLS's standard of care to business partners	
Enter into confidentiality agreements drafted by legal counsel with any organization that has access to MLS information systems	
Enter into information licensing agreements, drafted by legal counsel, only after specific authorization from the information owner	
Ensure that current license agreements exist for all software programs installed on MLS owned and operated systems	
Inspect the security provisions of Internet Services Providers (ISPs) and other third parties and contractors	

The rights of a business partner to use or repurpose member information should be defined at the time the information is created. The rights associated with many forms of MLS information, such as publications, should be described on documents, printed information, or published materials.

Digital information, more so than printed information, is vulnerable to unauthorized copying, repackaging, and theft. It is especially important that MLS executives ensure that they do not violate the copyright protections of third-party information they use in their business. MLS organizations should specify contractually the rights associated with the digital information. License agreements should define the rights of the recipient to

render the information that is printed in hard copy, viewed on a dynamic display, or played on an audio/video device

transport the information that may be copied, moved, or loaned

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

MLS executives 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 All Sensitive Information

Many forms of MLS information continue to exist on paper that must be physically secured. Access to property listings, research, contracts, and business 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 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, especially when the office is vacated.

MLS executives are responsible for ensuring that sensitive information under their control is not compromised through unauthorized access, editing, or manipulation. Confidential documents and sensitive information can be compromised and tampered with when transmitting the information or 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 locked screen savers when not in use. MLS organizations 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 by an employee or member should be subject to disciplinary action.

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

14. Community Outreach

MLS executives should help create and maintain an organizational culture that practices and values security and successfully communicates this to employees, contractors, partners, and members. Each individual who is given access to MLS information resources holds a position of trust and should be required to preserve security, protect member resources, and report violations of MLS policy. Technology and other active measures can help create, enforce, and maintain this culture.

MLS organizations should ensure their members use mature security technologies that are available to reduce the risks to community information. MLSs should concentrate their efforts on preventing unauthorized access and use by adhering to the following technology best practices:

Technology Best Practice	Assessment
Install firewall software on systems and personal computers	
Install and updating virus scanning and protection software	
Install intrusion detection at the network, host, and application levels	
Use a secure virtual private network 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 MLSs 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 an MLS 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 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. Securing Systems and Facilities

Many MLSs manage and operate information systems and facilities. This responsibility requires that policies, practices, and procedures are in place for their secure operation, whether they are “in-house” or “outsourced” to service providers. Best practices include the following:

- 15.1 Change Control Process**
- 15.2 Test Environment**
- 15.3 Software Protection and Control**
- 15.4 Network Management, Controls, and Operations**
- 15.5 Segregation of Duties**
- 15.6 Facility Management Oversight**
- 15.7 Procedures Documentation**
- 15.8 Records Management and Retention**

15.1 Change Control Process

MLS organizations periodically require system changes that should be documented and tracked to ensure that the impact on critical business operations is minimized and inadvertent damage is prevented. An effective change control process includes the following:

Change Control Process Best Practices	Assessment
Change Justification – MLS managers should ensure that the proposed change is necessary and that the change will result in better processes, procedures, or functionality.	
Nonproduction Testing – MLS managers should implement the proposed change in a nonproduction environment (e.g., test laboratory) to validate that the change behaves as expected.	
Functionality Testing – MLS managers should perform functionality tests that include a representative sampling of cause and effect behavior under which the component is expected to function. Testing should be performed against the nonproduction environment as well as the production environment after the change is implemented.	
Backup – MLS managers should perform backup of critical	

system data and previous-state data prior to change implementation.	
Contingency Planning – MLS managers should perform a sufficient level of backup or image preservation of the operational target environment in the event that the change does not function as expected and the previous state must be restored.	
Documentation – MLS managers should develop a detailed test plan and document each step of the change process in order to maintain test repeatability.	
Communication – MLS managers should inform all users who may be affected by outage or effects of the change prior to the change taking place. This notification also serves as a warning to those in charge of critical systems or business processes, which might not have been considered during the planning process and may be affected by a service outage.	
Scheduling – MLS managers should perform system changes when the least amount of impact to business operations is expected. This is typically after operational duty hours.	

15.2 Test Environment

MLS operations managers should ensure that the computing environment used to test upgrades and new software is well maintained. Development and testing performed within the production environment may affect the integrity of the system and user data. Therefore, any test or development activity should be performed in a segregated and/or isolated test environment (e.g., test laboratory). Advanced planning should ensure the availability and capacity of computing and systems resources. This should reduce the risk of system overload and minimize the chance of system resources becoming unavailable because of component failure. MLS managers should consider the following practices:

Test Environment Best Practices	Assessment
Software Development – All software development should be performed within isolated test environments and on dedicated development workstations, separate from the production environment.	
Executable Code – Executable code should not be implemented on operational systems until evidence of successful testing and user acceptance is obtained.	
Audit Data – An audit log of all updates to operational program libraries should be maintained.	
Contingency Planning – Previous versions of software	

should be retained for contingency purposes.	
Critical System Utilities – Compilers, editors, and other system utilities should not be openly accessible on operational systems.	
Authentication – Different log-on procedures should be used for operational and test systems to reduce the risk of confusion. Users should use different passwords for these systems, and menus should display appropriate identification messages.	
Requirements Analysis – Advance planning and preparation is required to ensure new or modified systems have adequate security, capacity, and resources to meet the present and future requirements. The operational requirements may be established, documented, and tested prior to acceptance of the system.	
Communication – For major new developments, operations staff should be consulted at all stages in the development process to ensure the operational efficiency and maintainability of the proposed system design.	
<p>Security Requirements – All proposals for new systems should include a security plan that describes how the system satisfies the security requirements provided in this document and any other applicable security policy definitions. At a minimum, the system design document should include</p> <ul style="list-style-type: none"> • Description of security functionality. • Minimum performance requirements • Optimal performance requirements • Capacity requirements 	
Nonintrusive Integration – All new application proposals should include evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times such as month end. Alternatively, they should include provisions for additional equipment to maintain adequate resource levels.	
Performance Monitoring – All information systems should be subject to an ongoing performance monitoring and auditing regime. The measurement metrics should be agreed to before the system is commissioned and should cover such aspects as system processing speed, capacity, and security performance. Acceptable levels of service should be negotiated at least annually with users and/or third-party service providers.	

15.3 Software Protection and Control

MLS operations managers should ensure that all information systems are adequately protected from malicious software by utilizing virus

prevention mechanisms. This applies to all organizational systems. Malicious software protection practices include the following:

Software Protection Best Practices	Assessment
Detection – MLS managers should ensure that all workstations, e-mail gateways, and multiuser systems are equipped with virus prevention software	
Update – MLS managers should ensure that each instance of virus prevention software is configured for automatic updates of the virus signature database. This may be performed via centralized organizational virus update server or directly from the product vendor.	
Unauthorized Software – The use of software not authorized by MLS managers should be prohibited.	
Questionable Media – All discs and electronic files of uncertain or unauthorized origin should be checked for viruses before use.	
Use of antivirus Software – Users should not tamper with or otherwise affect the normal operation of antivirus software without authorization. Change requests may be submitted to MLS managers prior to modification or configuration of antivirus software.	
Reporting – Users should report all instances of malicious software detected to the appropriate organizational agent (e.g., help desk, information security staff).	

15.4 Network Management, Controls, and Operations

Managers should implement the following controls to ensure the safeguarding of information being transmitted by networks and protection of the supporting infrastructure:

Network Management Controls Best Practices	Assessment
Separate the operational responsibility for networks from computer operations where appropriate.	
Establish responsibilities and procedures for the management of remote equipment, including equipment in user areas.	
Establish special controls to safeguard the confidentiality and integrity of data passing over public networks and to protect the connected systems. Special controls should also be required to maintain the availability of the network services and computers connected.	
Coordinate management activities to both optimize the service to the business and to ensure that controls are consistently applied across the network infrastructure.	

When choosing and deploying Real Estate Transaction Standards (RETS) servers, MLSs 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). MLSs should take care to ensure their RETS server vendor is not bypassing local MLS data access policy, but rather supporting and implementing policy.	
--	--

15.5 Segregation of Duties

Segregation of duties should reduce the risk of accidental or deliberate system misuse. MLS managers should identify critical roles and processes where fraud or misuse would cause significant damage to the organization or its members.

Segregation of Duties Best Practices	Assessment
MLS managers should separate the execution of an event from its authorization in order to reduce opportunities for unauthorized modification or misuse of information or services.	
In situations where separation of duties is impractical, MLS managers should establish monitoring processes to minimize the possibility that a single person can perpetrate fraud or misuse. Methods include increased audit or logging capabilities, management supervision, or involving multiple parties in activity validation (e.g., checks and balances).	

15.6 Facility Management Oversight

MLS managers should identify risks associated with the use of an external contractor to manage systems operations and facilities. Such risks may lead to security exposures at the external site. MLS managers should coordinate with the contractor or facilities manager to review requirements, identify risks, and ensure that appropriate controls are feasible and incorporated into service level agreements. Best practices include:

Facility Management Oversight Best Practices	Assessment
Identify sensitive or critical applications and determining the location (in-house or at external facility) best suited to meet systems operations requirements	
Obtain the approval of business application and data	

owners	
Document the business continuity plans	
Include security standards and the process for measuring compliance in all service level agreements	
Assign specific security oversight responsibilities and procedures to MLS employees to ensure vendor compliance	

15.7 Procedures Documentation

MLS managers should ensure that operating procedures specifying the organization's security policy are documented and maintained. Operating procedures should be treated as formal documents and with changes authorized only by management. These procedures should define the tasks associated with each job within the systems operations facility. Best practices include documenting the following:

Procedures Documentation Best Practices	Assessment
Job descriptions, including security authorization for all employees and contractor staff	
Scheduling requirements, including interdependencies with other systems, earliest job start, and latest job completion times	
Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities	
Support contacts in the event of unexpected operational or technical difficulties	
Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs	
System restart and recovery procedures for use in the event of system failure	
Housekeeping activities, including computer start-up and shutdown procedures, backup, equipment maintenance, and computer room and mail handling management	

15.8 Records Management and Retention

MLS operations managers should institute records management controls over the creation, use, and maintenance of records that track organization performance. Best practices include the following:

Records Management Best Practices	Assessment
Retention – MLS managers should define a retention period (either required by law or by organizational policy, which exceeds relevant legal requirement).	
Accessibility – All operational records, regardless of format or medium, should be organized, classified, and described to ensure their effective use during an audit of performance evaluation.	
Availability – All records should be made available for use by all appropriate organizational staff for their authorized retention period.	

MLS managers should also ensure the authorized disposition of records, regardless of format or medium. Permanent records should be preserved, while temporary records no longer of use should be promptly and securely deleted or disposed of when their required retention period expires, in accordance with member-approved records retention policies.

16. Securing End User Applications

MLS managers provide employees and users from many organizations with end user application support including the following:

- 16.1 E-mail**
- 16.2 Desktop Systems**
- 16.3 Public Access Sites**
- 16.4 Wireless Communications**

16.1 E-mail

This application is a primary vulnerability due to communications that can be intercepted and the unauthorized transfer and indiscriminate redistribution of member information. MLS organizations can minimize these risks by implementing the following best practices:

E-mail Protection Best Practices	Assessment
Encryption – MLS managers should provide users with the means and training to encrypt and decrypt e-mail. This can be performed with built-in encryption mechanisms that utilize a local public-key database, or with a third-party	

mechanism that requires a remote user's public key, self-decrypting archive utility, or manual cut-and-paste encryption.	
Nonrepudiation – MLS managers should provide users with the means to apply digital signatures to transmitted e-mail. This will provide a high degree of assurance that messages transmitted from a particular user actually originated from the user.	
Digital Signatures – MLS users should utilize the MLS-provided utilities for encryption and application of digital signatures to transmitted e-mail of sensitive information.	
<p>When sending potentially sensitive e-mail to users for whom the sender does not have a public key, MLS users should ensure that the data is protected. Methods may include</p> <ul style="list-style-type: none"> • Sending self-decrypting archive, using a robust pass phrase • Requesting from the remote user a public key with which to encrypt the data • Other means besides e-mail 	
<p>Prohibited Use – Users should not use e-mail for the purposes listed below. Users who receive any e-mails with this content from any Realtor® organization employee should report the matter to a Realtor® manager immediately:</p> <ul style="list-style-type: none"> • Creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin • Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam) • Any form of harassment via e-mail, whether through language, frequency, or size of messages • Unauthorized use, or forging, of e-mail header information • Solicitation of e-mail for any e-mail address other than those of the sender's accounts • Creating or forwarding "chain letters" or other "pyramid" schemes of any type • Use of unsolicited e-mail originating within organizational networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the organization or connected via the organizational network • Posting the same or similar nonbusiness-related messages to large numbers of Usenet 	

newsgroups (newsgroup spam)	
Personal Use – MLS users should be permitted a reasonable amount of organizational resources for personal e-mails, but nonwork-related e-mail should be saved in a separate folder from work-related e-mail. REALTOR® managers should approve virus or other warnings and mass mailings from the organization. These restrictions also apply to the forwarding of mail received by other organizational members.	
Monitoring – MLS users should have no expectation of privacy in anything they store, send, or receive on the organizational e-mail system. MLS managers may monitor messages without prior notice.	

16.2 Desktop Systems

MLS operations managers should ensure that activities performed on member organization workstations do not negatively affect organizational resources, compromise security measures, or impact network stability. Best practices include the following:

Desktop Systems Best Practices	Assessment
<p>Standardization – MLS managers should ensure that office systems are built, ordered, or configured based on a common profile. At a minimum, profile specifications include</p> <ul style="list-style-type: none"> • Approved and common hardware configurations • Approved and common operating systems and software • Common access control configuration • Automated management processes including virus protection, software updates, and system performance monitoring 	
<p>Prohibited Activities – MLS users should be prohibited from performing the following activities and MLS managers should monitor and audit all systems operations to prevent and contain:</p> <ul style="list-style-type: none"> • Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan Horses, e-mail bombs). • Creating security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, 	

<p>network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.</p> <ul style="list-style-type: none"> • Port scanning or security scanning is expressly prohibited unless prior notification to organizational management is made. • Executing any form of network monitoring that will intercept data not intended for the employee's host. • Circumventing user authentication or security of any host, network, or account. • Interfering with or denying service to any user other than the employee's host (e.g., denial-of-service attack). • Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet. • Installing any additional hardware or software or altering any operating system or application security settings. • Installing modems or other communications devices on computers connected to an organizational LAN. • Abusing network bandwidth by accessing streaming video or audio. 	
--	--

16.3 Public Access Sites

MLSs that provide public access to listings information through Web sites, including IDX and VOWs, are at risk of disclosing sensitive information. Best practices include the following:

Public Access Best Practices	Assessment
<p>Content Management – MLS managers should define requirements for third-party providers of software and content that is resistant to attack, requirements to include</p> <ul style="list-style-type: none"> • Front-end, public-accessible scripts, • Middleware and database applications, and • Scripts and processes that provide for component interconnection. 	
<p>Security Testing– MLS managers should perform or coordinate security testing against public access sites and to maintain an acceptable level of protection. Testing should include</p> <ul style="list-style-type: none"> • Preproduction user testing to ensure functionality and usability 	

<ul style="list-style-type: none"> • Preproduction security testing to validate security requirements and identify problems prior to production • Impartial (externally performed) postproduction security testing to validate security requirements • Periodic reevaluation of portal security to evaluate security based on changes in the operating environment 	
<p>Site Security – MLS managers should implement security measures to protect the confidentiality and integrity of the public access portal and the supporting infrastructure including</p> <ul style="list-style-type: none"> • Access to the published content should not allow unintended access to networks or devices to which it is connected. • Custodians of public access portals should provide sufficient protection to prevent unauthorized modification or configuration of electronically published information on the public access system on which the information resides. • Users who access public content should be authenticated to an assurance level based on the sensitivity of the information they access. Any confidential information available via the Internet should be accessed only after authentication of a user identity. • Authentication of identity should be accomplished through verification of consumer registration information through either real-time or out-of-band processes. 	
<p>Rights Approval – MLS managers should obtain publication approval for content that is made publicly accessible. All information to be made publicly accessible should be considered for the following:</p> <ul style="list-style-type: none"> • Application of appropriate security classification prior to publishing. • Content compliance with laws, rules, and regulations in the jurisdiction in which the system is located. • Formal authorization process of all data prior to publishing. • Information requiring an assurance of integrity, made available on a publicly available system, should be protected by appropriate mechanisms (e.g., encryption). • Content requiring persistent protection through multiple distribution partners should be protected through digital rights management capabilities. 	

16.4 Wireless Communications

Improperly installed or configured wireless access points are a major security risk, potentially exposing the entirety of the communications and information resources of the MLSs 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 MLS offices without the authorization and assistance of the MLS 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 VPN.

17. Responding to an Event

The effective implementation of best information security practices can prevent or reduce serious business losses or disruption. Despite the MLS'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 will help minimize the disruption to your business and the potential for business loss.

Continuity Planning Best Practice	Assessment
Plan – MLS managers should establish procedures to document, maintain, detect, and establish the cause of security incidences.	
Respond – MLS managers should define the corrective action to be taken in response to incidents in order to prevent or minimize recurrence.	
Quality Control – MLS managers should establish review procedures to monitor the implementation and effectiveness of any corrective action, including any required changes to existing procedures.	

Incident response procedures should be published and staff trained with responsibilities delegated as appropriate. Whether an incident is minor or major, it should be reported and handled properly. An improperly handled incident can result in lost data or resources.

MLS executives should establish an escalation path that indicates who is responsible (i.e., point of contact) for various levels of incidents. The escalation path should include secondary and tertiary points of contact if the primary is not available. MLS executives should make the escalation path known to all members of the organization.

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 assets. Whether an incident is minor or major, it should be reported to the security manager for proper handling. Escalation procedures may vary based on the severity of the incident as follows

Reporting Best Practice	Assessment
Minor Incident – Initial stage of incident response reporting should involve help desk personnel. The help desk personnel should be suited to address the incident or escalate it to the appropriate MLS manager.	
Moderate Incident – The security manager should become involved to address incidents that require the involvement of information security personnel.	
Serious Incident – If information security personnel are unavailable or not suited to address the incident, MLS managers should take the appropriate actions required to address the incident, including reporting it to law enforcement. Incidents that may require law enforcement involvement include embezzlement, fraud, theft, and similar crimes.	

The cornerstone of the business continuity plan is ensuring that critical business documents and a current version of any electronic media have been securely stored off-site, away from your place of business. Copies of applications that have been custom developed or modified should also be stored off-site and readily available. Business applications utilizing commercial, off-the-shelf software can generally be restored quickly once new computing resources and backup data files are obtained.

MLS managers should ensure that adequate backup and recovery procedures are developed and enforced. Adequate backup facilities should be provided to ensure that all essential business data and software are recovered following an event or media failure. At a minimum, the following practices should be implemented:

Backup Best Practices	Readiness
<p>Backup Controls – Data administration should ensure that at least three generations of backup data are retained for critical business applications. Data administrators should establish and formally document an appropriate schedule of full and incremental backups.</p>	
<p>Remote Storage – Data administrators should ensure that a minimum level of backup information, together with accurate and complete records of the backup copies, should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.</p>	
<p>Data Protection – Data administrators should ensure that backup data is given an adequate level of physical and environmental protection, consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the backup site.</p>	
<p>Data Viability – Data administrators should ensure that backup data is regularly checked to ensure that it can be relied upon in an emergency.</p>	
<p>Data Retention –Data owners should retain data for the period necessary to satisfy both business and legal requirements. Data owners should identify the retention period for essential business data and should establish any requirement for archive copies to be retained.</p>	

MLS managers should ensure that procedures and guidelines are developed to sufficiently enable responders to handle and properly recover from incidents. In addition, all organization members should be trained on the procedures involving the proper handling of an incident.

Recovery Best Practices	Assessment
<p>Incident Handling – Incident responders should develop handling procedures for each system to address system failures, loss of service, and errors resulting from breaches of security. These procedures should be compatible with business continuity plan procedures and include</p> <ul style="list-style-type: none"> • Analysis and identification of the cause of the incident • Planning and implementation of remedies to prevent recurrence 	

<ul style="list-style-type: none"> • Collection of evidence, such as activity logs, for analysis • Communication with business users and others affected by, or involved with, recovery from the incident 	
<p>Incident Recovery – Incident responders should perform recovery from incidents in a manner that preserves evidence and if possible keeps critical systems available. Priorities in the recovery process include the following:</p> <ul style="list-style-type: none"> • Only authorized individuals are allowed access to live systems and data. • All emergency actions taken are documented in detail and reported to management. • The integrity of business systems and security controls is confirmed with minimal delay. 	
<p>Organization Training – Managers should provide all organizational members with procedures involving the proper handling of an incident.</p> <ul style="list-style-type: none"> • Those who encounter an incident should report the incident in a timely fashion. • All evidence should be considered fragile and volatile in order to maintain the evidence’s admissibility (for use in possible litigation) and viability (for use by investigators to determine cause). 	

18. 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. MLS executives should establish a training and education program for staff that use, administer, and maintain sensitive information and systems. These programs should include the following best practices:

Education Best Practice	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 30 days of being granted access to any system or	

information resource.	
Update all users on the local, state, and national policies that may affect the protection of Realtor® information.	
Ensure that incident response procedures are included in the training program. Procedures should be published, the staff trained, and responsibilities delegated.	

19. A Community Responsibility

The need for members to preserve consumer privacy, protect business critical information, and control the point of sale will continue to grow.

The Internet created a major shift in the way practitioners collect and make listing information available to consumers. The next major shift will involve how all forms of broker and MLS 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 member efforts to remain as the “trusted” first point of consumer contact requires that MLS executives continue to work to improve the information security procedures and technology protections of their members’ information and their operations.

Though industry business models, participants, regulation, threats, and technology will continue to change, information security will remain a mandatory requirement 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. However, the promise of greater convenience and service quality must include preservation of consumer privacy and control of broker and MLS information.

MLS executives have a vital role to play in the evolution of the industry’s information security governance, management, and technology info-structure. 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 these practitioners 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 this or any information security topic, refer to the Realtor® Information Security Guidelines.