CMLS | Council of Multiple Listing Services

TECHNICAL AND IT **BEST PRACTICES**

CMLS BEST PRACTICES GUIDE FOR THE MLS

CMLS Best Practices bring together emerging and proven practices from across real estate to align and advance professional standards within the MLS industry.

Published By:
Council of Multiple Listing Services
1000 N. Green Valley Parkway #440-583
Henderson, Nevada 89074
cmls.org / 877.505.8805


SMS
CMLS

BACKGROUND

CMLS Best Practices began as a work group initiative that grew out of an idea submitted in 2013. From that initial workshop spark, the group curated the best ideas submitted by attendees, added policies and procedures gathered from CMLS members, and recruited Ann Bailey of Pranix Inc. to refine, organize, and add further insights. The result was the publication of seven documents capable of guiding any MLS organization to meet industry standards and recognized benchmarks.

The objective of these documents is to help MLSs of all sizes make the market work by encouraging them to adopt the best practices of a community that consists of leading MLSs and business partners. In sum, best practices help MLSs and subscribers succeed.

In an effort to keep pace with a rapidly changing marketplace, CMLS began work on a newly updated set of comprehensive documents that would help MLSs deliver the tools, tactics, and technologies their customers need.

The result was the creation and publication of the Technical and IT Best Practices document, a guide that retains proven strategies while providing additional insight into emerging technical and informational technology. Its development was spearheaded by the CMLS Technical and IT Section Council and numerous contributing organizations referenced at the end of the document.

DEVELOPMENT

More than a dozen contributing organizations and countless MLS professionals are responsible for the development of the Technical and IT Best Practices Guide. For a full list of contributors providing research, insight, and authorship, please see the references page at the end of the guide. Thank you.

CONTENTS

OVERVIEW

While there is no single technology standard that can be considered a best practice for the entirety of the multiple listing services industry, every organization within the industry can benefit from the review, recognization and application of reasonable guidelines across their technical and IT operations. This guide presents strategies and concepts for various aspects of technical operations and management.

By applying many of these recognized principles of accountability, everyone benefits — MLSs, their customers, and the communities in which they operate. Such clear guidance in technology goes a long way in fostering a fundamental confidence in the real estate market.

TECHNICAL MANAGEMENT

Most organizations employ many different systems to support various business activities. These systems include the obvious — phone systems and services, multi-function printers, networks, computers, mobile devices — and the not-so-obvious — automated support systems. Together, these systems work like an organization's nervous system, connecting it to an internal infrastructure and the external world and promoting its ability to be productive, responsive, and profitable. It is essential for the organization's health, risk management, and legal or policy compliance.

This is why information technology (IT) is referenced inside any organization. IT is the application of computers, peripherals, software, and telecommunications equipment to store, retrieve, transmit, analyze, and manipulate data; often in the context of a business or other enterprise. The term is commonly used as a synonym for computers and computer networks, but encompasses much more.

There are several key areas that determine the success of IT services. These include:

- **Planning/Budgeting.** Provide continuity, respond to current situations, guide leadership and management decisions, and meet evolving business needs.
- **Operations.** Maintain appropriate housekeeping procedures to assure security, productivity, and compliance.
- **Fulfillment.** Provide the necessary hardware systems and software to support staff and deliver a superior product with excellent customer service and training.

Within this framework, each organization should tailor the issues to meet its business plan, physical resources, and any budgetary constraints or priorities. For further consideration, see "The Ten Commandments of Computerization" published by The Canadian Association of Information Technology Professionals. The article broadly applies to the discussion of technology best practices and augments several other models highlighted throughout the guide.

Practice 1. Develop a plan to allocate resources that meet organizational needs.

Practice 2. Define the roles and relationships of staff and outside partners.

Practice 3. Assign clear responsibilities for the maintenance of internal systems.

Practice 4. Add outside service partners when their expertise is needed.

Practice 5. Work with leadership and partners to direct the execution of the plan.

Goals And Planning

Since all organizations have different skill sets and resources, it is important to assess the available talent, time, and budget of an organization along with any overall technical goals.

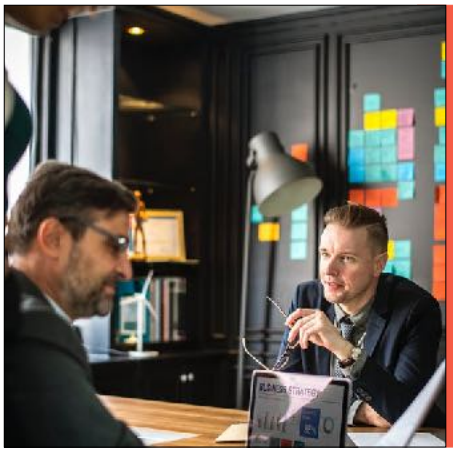
Smaller organizations, for example, will likely manage a network of computers with Internet access, accounting/customer software, telephone services, and an MLS software vendor/partner. They will likely be managed by staff with support from outside service providers: telecommunications, repair, maintenance, and operation.

Larger organizations have of all these systems and others. They may often be managed by a separate technical staff with responsibility for internal operations, system maintenance, and the management of outside service partners. Outside service partners may include software developers, system providers, web hosts, cloud software services, data center managers, and others.

Mission Critical Systems

Many of the internal and external systems will be considered critical to the operation of the organization. This will likely include data (customer and business information), communications (telephones and networks), hardware (servers), and software (accounting and multiple listing services).

As a result, these systems require an additional plan — one that assures their continued survival and operation during an emergency or service interruption. As an additional measure, any defined and associated risks can also be managed internally, insured, and/or assigned to business partners as necessary.



Mission Critical Planning In Four Steps

Step 1. Identify and document all systems within the organization.

Step 2. Develop plans for systems support and maintenance.

Step 3. Implement a formal and proven disaster plan.

Step 4. Test the disaster plan every year.

Disaster Planning

In the event of a natural or other disaster or service interruption, critical systems should be protected by a disaster plan that guides the management of the problem(s) and restoration of any services and systems. This plan will prioritize mission critical systems, define the processes necessary to repair or restore systems to normal, and identify the individuals/business partners responsible for action.

These plans should also include any temporary or stopgap measures that back up mission critical systems and ensure the operation of any critical components. Any scenarios that are developed should be tested periodically to ensure that mechanical systems work, the responsible individuals know their roles, and that systems can be restored as expected. A post-test assessment will help the organization better understand what occurred, what worked, and what could be improved.

These various scenarios should also be prepared before any event occurs. Most organizations start with a brainstorming session to identify any situations that could occur and the actions that need to be taken to restore normal operations as quickly as possible.

Most organizations will also include any communication specialists in the development of the plan. Communication among business partners, staff, and customers is always critical to success and full recovery.

Budgeting and Expenditures

Technology is a moving target. Budget plans must be put in place to fund current operations, commitments, and maintenance as well as improvement upgrades and replacements. Income, expense, and capital are all part of the fiscal planning cycle.

In larger organizations, IT departments are responsible for developing a budget proposal. Smaller organizations without an IT department may rely on management or volunteer leadership. Either way, the organization should consider its obligation to remain current and competitive but not necessarily on the "bleeding edge" of technology or engage in any activities outside of its competence, or that of its staff, leadership, partners, or customers.

At the same time, there is always a business interest to be progressive and competitive and demonstrate both to customers. While customer wants and needs should be part of the planning process, they should not drive product and service delivery toward short-term solutions.

Technical Budget Best Practices In Three Steps

Step 1. Consider ongoing capital investments.

Step 2. Clearly identify income and expense for tech activities.

Step 3. Evaluate financial impact for internal staff vs. outsourcing.

The balance is often found in that agile software development and lean business processes are effective tools. Agile management or project management is an iterative and incremental method of managing the design and build activities for engineering, information technology, and new product or service development projects in a highly flexible and interactive manner, such as agile software development.

Such ongoing planning and business cycles take customer needs into account, the products and services available in the market, and the advancement of the organization's business. When considered together, management is better able to make smart financial decisions in regard to technological improvements, upgrades, repairs, and investments.

Along with these considerations, some special attention should be given to internal and external activities as well as resource requirements. Sometimes, findings in either area can provide additional insight that will help the organization better align its resources.

Internal vs. External Activities

Staffing for all of the activities and systems identified in the planning can be internal or external. Careful consideration should be given to each element of risk, expense, talent and facilities. Even experienced organizations choose to retain business partners that specialize in various critical efforts.

Much as most companies do not choose to repair and maintain their own copiers and printers beyond replacing toner and paper, similar consideration should be given to systems.

Most MLS software systems are hosted on the vendor's networks and servers, which often means the performance, backups, and maintenance are the responsibility of the system vendor. Some organizations may still choose to host such systems internally and have staff take on the risks and responsibility for operations, but the cost to develop and maintain data centers of any size is becoming a specialty better served with shared costs and risks.

Conversely, some data centers can be maintained internally with computer systems that can be hosted in a co-location facility or virtualized in the cloud. Along with those systems, software is often a service (SaaS)[1], a way of delivering applications over the Internet. This leaves the responsibility for maintenance and ongoing feature enhancement to the vendor.

Resource Requirements

To determine the best resource requirements, a plan should be developed to allocate available resources to meet the organization's needs. Working with leadership and business partners, staff can define and direct the ongoing execution of the plan.

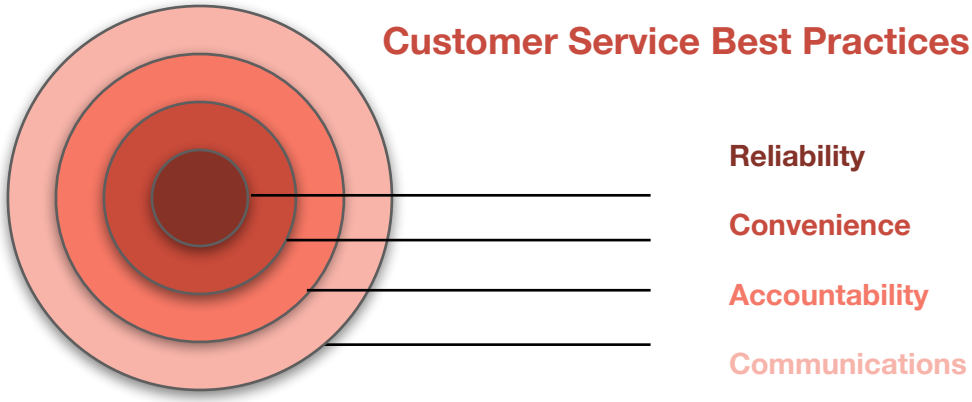
Mission critical systems are usually identified in these plans as well as their support and maintenance. Single points of failure should also be identified with a plan to rectify as well as the allocation of redundant systems.

The organization's budget process should also include (and clearly identify) income, expense for technical activities, and ongoing capital investments. The roles reserved by the organization's staff and roles contracted out with partners should be identified, along with any relationships that are critical to the success of all technical systems.

1. Software as a service (SaaS) is a way of delivering applications over the Internet as a service. Instead of installing and maintaining software, companies simply access it via the Internet, freeing themselves from complex software and hardware management. Saleforce.com is one example.

OPERATIONS

There are many aspects to the services that an organization requires internally or provides to its customers in the course of its business. A feedback cycle of information that consists of Customer Relationship Management (CRM), training and support will provide improvements for the customer. The objectives are always the same — reliability, convenience, accountability, and communications.



Larger organizations will have the resources to assign these technical management responsibilities to a chief technology officer (CTO) or chief information officer (CIO). Smaller organizations may augment limited staff resources with outside services and business partners. Regardless of how these responsibilities are managed, best practices require the development of policies and procedures that document general operations, specific business activities, and assignment of various responsibilities.

Support Staff, Training, and Services

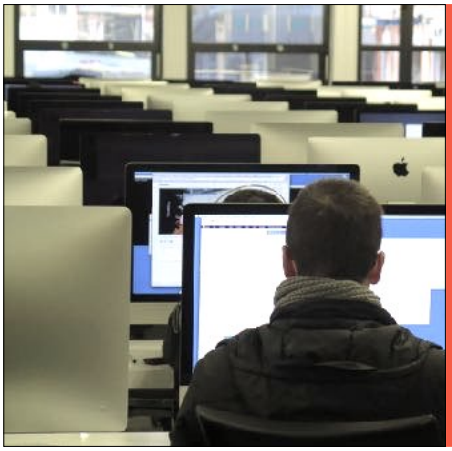
The successful execution of operations requires a well trained staff and educated customer base. Effective organizations create, develop, and implement a variety of education program for members and staff.

Support staff training. The organization is responsible for staff training to support its systems. Management must evaluate employee needs and aptitudes and then provide appropriate training and support. Depending on the size of the organization, specific staff may have general responsibilities for software, hardware and other more complex systems. For example, a “key operator” is often assigned the responsibility of managing systems such as telephones, copiers and printers.

Training on some systems may also be assigned to vendors. Such responsibilities should be clearly documented and communicated throughout the organization.

Member education. Many organizations provide support staff and training at customer locations or local association offices. Training is typically provided along with new systems or after updates to existing systems. Most presenters use standard equipment, including laptops, tablets, LCD projectors, and Wi-Fi connections. Some encourage customers to use their own equipment, allowing for active participation during the presentation.

Some associations and MLSs provide extensive education opportunities at formal training centers in addition to remote or web-based presentations. A training center may support multiple products or services, all of which are hosted on a network, located in a secure facility, and associated peripheral equipment such as printers. The equipment, not the content, is a technical responsibility.



Technical Training and Education Best Practices

Step 1. Develop environments for education and training.

Step 2. Utilize technology solutions for education.

Step 3. Develop ongoing support and communication.

Web-Based services. Integrated web-based programs and webinars are an increasingly important part of customer service and support. The technical aspects of these activities include the installation, setup, and maintenance of software and hardware. It may also include all necessary network support for production, deployment, and presentation.

Business meetings are also often conducted by means of the same web-based services used for training. They often integrate telecommunications (or VoIP), video, and documentation. Technical services usually supports telecommunications and network connections, including additional security as needed.

More importantly, technical services should become engaged participants who seek out systems and develop education and training programs that help:

- **Fulfill staff duties**
- **Enrich staff experience**
- **Support customer relations**
- **Improve business interactions**

Documentation

With the development of successful procedures and practices, institutional knowledge becomes an increasingly critical component of any organization. Unfortunately, it is also very often a notable weakness in most organizations. The solution is documentation.

Documentation provides a clear set of guidelines for how certain activities are conducted, the accountability that necessary steps are consistently followed, and a manual for continuity within the organization. Such documentation should be created to track activities and problems, manage similar projects, and define regularly conducted tasks.

The concept of the Wikipedia website, for example, has been expanded to provide an environment for team communication and collaboration as well as general documentation. It can be updated regularly, include dynamic references, and allow multiple users.

Some activities, such as Payment Card Industry (PCI) compliance, International Standards Organization (ISO) certifications or RESO require very detailed documentation of the steps taken for related tasks — who does what and when, where data is stored and secured, and how systems (both human and electronic) relate to each other and produce expected outcomes.

Both software and hardware systems will require documentation. Sufficient system-specific documentation should be created and maintained to assure continuity in the event of staff or vendor turnover and the restoration of systems in the event of a problem. Documentation is also beneficial for the maintenance of ongoing systems and planning purposes. Some computer code will provide its own documentation. Some may require IT to provide such documentation, especially if it is complex.

This documentation must be maintained in a central location or web-based or other cloud service. Information that is carried in someone's head, on a personal smart phone, or one person's office is not considered proper documentation. Likewise, neglected documentation that is not backed up is the same as having no documentation at all.

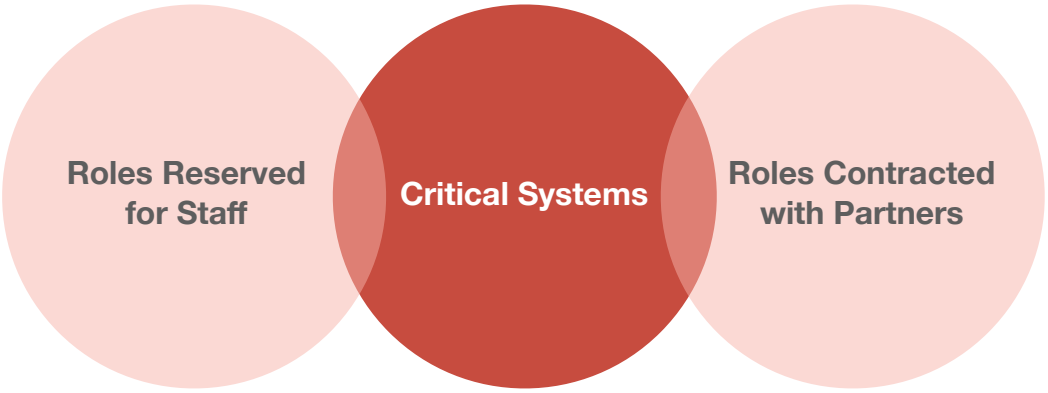
Users (customers, staff, and volunteer leadership) are notorious for not referring to written documentation, including online references. This is why the training and support staff will look at a variety of delivery methods for their messages. This includes context-sensitive help, printed and online reference materials and examples, and knowledge bases that build on the shared community experience and expertise. The various methods make the information available for specific inquiries, good management and general compliance.

Outsourcing

Almost all organizations outsource some systems and services because it allows an organization to shift workloads, focus on core competence, or acquire additional expertise and talent that is does not possess or desire to acquire. Instead, relationships are developed with trusted business partners to respond and provide services such as maintenance and repair, system development, or help line response.

Even if the organization outsources any system or service, it is still responsible for the evaluation and management of these relationships. It is also responsible to how these outsourced services will be coordinated or work in tandem with organization staff.

Decisions About Organizational Roles



As mentioned, consultants are frequently retained to provide technical advice and evaluations. Outside experience and knowledge may also provide additional support for implementation of the technical plan and goals.

It is a worthwhile engagement for the organization to have a technical consultant evaluate or audit systems for both compliance and currency — for existing systems as well as any potential acquisitions, system replacements, or business partner solutions. Such technical audits review the processes and systems in use within the organization (or under consideration) and report findings to management and to board leadership.

Common areas for review include: documentation, system segregation, staff roles (physical and logical), security, data management, backup, and recovery.

Consultants should always have well-defined specific roles and responsibilities. Their work is usually confined to specific purposes that are defined in a contract or letter of engagement. This document will also lay out the expected results and format of any recommendations or actions. One task for a consultant is a Request for Proposals (RFP) process that seeks and solicits software like an MLS or CRM system.

Typical Consultant Responsibilities

- Identification of business needs
- Identification of vendors with potential solutions
- Development of RFP, with requirements, timelines and contracts
- Review of responses and any follow-up inquiries
- Selection of possible providers and product demos
- Product selection by management or volunteer leadership

Other tasks taken by a consultant many also include business planning, competitive business reviews, and organizational restructuring. They may also provide experience or an objective outside view that will benefit an organization's review of its business operations, the environment in which it does business, and the development of the structure needed to support its business operations.

Regardless of the contract, however, the organization retains responsibility for the final analysis, all decisions, and execution of the consultant's recommendations or advice.

Policies

Policies are guidelines necessary to provide a framework for the management of systems and services for and by staff. The general concept behind writing a policy is to encourage best and proper use of the systems employed by the organization in its business activities.

These could include any number of systems: email systems, use of software owned or licensed by the company, and the personal or business use of networks and hardware (e.g., desktop or laptop computers, tablets, and smart phones). Policy examples might include that all emails, incoming and outgoing, are the property of the organization. Another policy might prohibit installation of unauthorized software on company computers or copying of software owned or licensed by the organization (this includes intellectual property owned by others but not licensed such as movies, MP3s, game servers, software, automatic license key generators, or illegal downloads). Another policy might outline daily or periodic activities such as data development, document retention, and backups.

Email and social media policies are especially important because it is a ubiquitous part of daily communications but only a portion of which may be of any particular value. For instance, spam and malware can be introduced to otherwise secure systems via email. Therefore, it is always a potential threat to networks and communication systems. This is why policies should define the purpose, privacy rights, and use of company email systems.

Many organizations operate in a partial or complete Wi-Fi environment, allowing connectivity from nearly anywhere. In the new world of "bring your own device" or BYOD, employees and customers frequently connect to networks with smart phones, tablets, computers, and other devices.

Having policies in place can guide employees on when, where, and how to connect to outside networks and how they or guests may connect to those networks operated by the organization as well. Policies can address any number of issues, including permissible uses, connection protocols, and security issues.

All networks should be segregated according to the user audience and any appropriate access limitations should be defined and enforced. Organizations may also choose to incorporate Virtual Private Networks (VPNs), which allow private networks to be extended over public Internet channels. While they provide additional convenience and security, they also require further policies and procedures.

Policies can also be written to provide software guidance as well. These policies could address the access, use, copying, installation, and security of all software owned by the organization. Contracts and service level agreements should be carefully negotiated and monitored for performance and compliance.

Failed agreements ultimately result in dissatisfied customers or unpleasant disputes. Legal issues such as compliance with the Digital Millennium Copyright Act (DMCA), general copyright, licensing, and trademark laws should be reviewed and addressed. Policies and guidelines for staff and customers should be developed in coordination with the organization's legal staff, which is addressed in depth by CMLS Legal Best Practices.

Websites And Online Services

Most organizations maintain one or more websites and social media accounts to communicate with customers, represent services and benefits, provide portals to software and solicit business, and establish an online identity. Ideally, any website should be identified as part of a goal-oriented plan or process that defines its features and content.

These plans should describe the goals of the website and provide an outline of the content that will be presented in a way that any volunteer leadership can understand and, perhaps, contribute to. It should be expected that, as a dynamic platform, most websites will require review and revision by staff on an ongoing basis.

Ideally, there should be an opportunity to solicit feedback from customers or other end-users. Such feedback is invaluable because it can improve content and features prior to the next update. In some cases, a website can also be maintained and hosted by a business partner. Even so, most website content and management is maintained by staff.

Domains and URLs are not only Internet addresses but also business identifiers. They should be protected and managed along with other intellectual property. Many organizations reserve multiple Top Level Domain (TLD) names and extensions that relate to their business, activities, regions, product names, and organizational names.

Social Media. In recent years, organizations have also begun using blogs and social networks to communicate with customers and other communities by providing information, engaging in public dialog, and gathering information. While the objectives and tactics of such activities are usually the responsibility of marketing and communication, any software or application programming interfaces (APIs) may remain the responsibility of IT services.

SECURITY AND DATA

An organization has an obligation to protect its systems and all the data that those systems contain or access. This process is best described as a variety of tactics and tools that are employed to prevent, identify, and resolve any breaches of the systems.

On some level, security is common sense. Successful organizations continually encourage and educate staff and customers on the need and benefits of security. And while there are cost/benefit thresholds that an organization should identify, the goal of any technical and IT team is to provide maximum security for a reasonable investment — decisions that may find human management and monitoring is more cost effective than some of the most sophisticated software solutions on the market.

General Security

Basic security is not limited to technical assets. It includes all the locks on the office doors and other perimeter defenses. Facilities are the first line of defense and should be resistant to strangers or any off-hour invasions.

Alarms should be installed and monitored for such things as open or broken windows, movement within spaces that should otherwise be vacant, temperatures in asset sensitive areas, and water where any would be unwelcome or dangerous. Likewise, fire protection should be provided as appropriate for the facility, including: extinguishers, sprinklers, and suppression systems.

Security systems providers can assess and advise on most needs and costs. Some organizations may even have secure areas that require identification or pass cards.

Aside from the facility, the first line of defense from Internet invasions are passwords, which may be assigned or left to the discretion of the employee or customer. In such instances when the employee or customer can create their own, guidelines for the complexity of the password should be established.

Avoid obvious combinations or personal information that could lead to a breach of the system in use. The strength of any password depends on its complexity, which includes a variety of characters and length of combination. For example: “Monday” is a weak password while “M0nday%34” is a stronger variation.

A longer password — eight or more characters — with varied case and non-letter characters is best. It is also best not to use the same password across multiple systems and to avoid commonly known information such as a user’s pet, family name, or other identifying description. The entire point is to create passwords that a trespasser cannot guess.

Typical Password Guidelines

- At least eight or more characters in length
- Contain at least one number and one upper case letter
- Should be unique and not used across multiple systems
- Cannot be repeated within 12 months or contain a “default”
- Need to be changed monthly or quarterly depending on data
- Should never be written down or shared with multiple people

Some systems may require more complex security for access such as secondary authentication. This process, for example, provides a user with a unique code/password to be entered following the user-supplied personal password. The unique code may be required by software or a device (fob or USB)[2] that generates a code, or a mechanism that supplies a code via a text message to a specific user while logging into the system. The banking industry requires substantial security procedures for employees who log in to corporate systems from remote and office locations.

Passwords and other security protocols can be managed. Devices are available that will securely store multiple passwords so that only one needs to be recalled to access the others. Software may be employed by the organization to store or record multiple passwords, seldom-used passwords, or shared passwords.

Single Sign On (SSO) provides a gateway to multiple related but independent systems and servers by means of a single password or code. The concept is to provide customers (or staff) with a single point of entry to allow greater ease of access without having to log on to each system. These SSO features may be provided by the technical staff, a business partner or vendor, or RESO Web API. Security Assertion Markup Language (SAML) along with OpenID and Oauth2 are common solutions for the exchange of user security between systems. User credentials are challenged and authenticated to provide access or services.

2. A universal serial bus (USB) flash drive is a small, portable device that plugs into a computer's USB port. Like a hard disk, a USB flash drive stores information and can easily transfer information.

Most systems have utility software designed to monitor their activity and any activity by those who access them. These activities are reported as metrics that should be monitored for how the various systems perform, who is accessing these systems, and how are the systems are being used.

Website monitoring also provides information about traffic and their audiences. Both management and leadership need to know this information and review it on a regular basis. The metrics will provide some measures of success for various systems as well as identify any problems as quickly as possible. Alarms and warnings built into the software will disclose any problems — unauthorized access or performance issues — allowing the organization to respond and resolve any issues. Many software features allow the systems to communicate incidents or problems directly to responsible staff or business partners any time they occur by means of text, email, or telephone.

Systems Security Best Practices

Practice 1. Security is a priority for any organization.

Practice 2. Physical security is the first line of defense.

Practice 3. Passwords must be complex per policy.

Practice 4. Systems must be monitored and tested.

Practice 5. Some systems require special isolation.

Practice 6. Threats must be resolved immediately.

Keep in mind that metrics may be different for different systems. There is no exhaustive list of which metrics are best matched to what systems. Organizations generally develop formats for statistics that provide them with the information they need to effectively manage their systems, evaluate the effectiveness of software and vendors, and report activity to leadership as requested. Software metrics may indicate what functions are being used by customers, when and for what areas, and as a measure for response times to customer requests.

New employees and new business partners will require an orientation to the security policies and procedures of the organization as relevant to their responsibilities. Existing employees should be provided regular refreshers on security, policy, and procedures. Likewise, departing employees require an additional degree of attention as appropriate to their departure, whether a resignation or dismissal. In such cases, the entire organization should respond and revise any and all passwords or codes to systems to which the previous employee may have had access. It is a technical responsibility to see that email accounts are disabled and hardware and software is accounted for.

Departing employees often are interviewed or processed through human resources who will have a checklist or documents to assist with the formal procedure. The employee is informed of their obligations and those of the organization at termination.

Tech Tip: Network metrics may indicate volumes of traffic by time of day, day of the week, bandwidth used, and bandwidth required. System metrics may provide statistics on usage, availability, access, and threats. Websites can be monitored for number and types of users, web pages viewed, location of the users, and other assigned metrics.

In today's world, physical security is insufficient given the sophistication or persistence of determined hackers, disgruntled employees, angry customers, or creative and curious teenagers. Software and hardware must be installed and configured to prevent intrusions, installation of malicious software or misappropriation of intellectual property.

Firewalls and Filters

Firewalls are set up to repel unauthorized access to networks. Most routers include a limited but somewhat effective firewall that can be configured to meet the needs of the organization. Larger systems and organizations tend to employ more complex firewalls specific to the systems they are protecting.

Managed firewall services and network security monitoring services can also be employed to augment staff in maintaining vigilance over network security. It is important they work in tandem with other system security. For example, spam filters can intercept nearly 99 percent of junk email, which is often one source of intrusion. With multiple systems, proper maintenance, periodic testing, and active metric monitoring, organizations can mitigate much of their overall risk.

Firewalls and security software can protect most systems from the majority of attacks, viruses, and inadvertent downloads. The objective is always to prevent an intrusion and any subsequent damage or service loss. Software can add a range of protections for spam, malware, viruses, and creative customers or staff. It can also provide encryptions when sent or received. It is still important that staff and business partners manage their activities to prevent intrusions. And, any breaches must be reported promptly and resolved to ensure that no damage has been done, minimize any chance that the incident will be repeated, and provide protections against secondary or similar attacks and unexpected affects on other systems.

Backups

The regular replication of software and data and storage in a secure location doesn't sound important until there is an emergency. Like an insurance policy, backups that are appropriate to a variety of situations should be in place. While everyone hopes they will never be needed, the time, effort, and cost of restoration is not inconsequential.

Backup best practices include that they should be performed in many ways and on different schedules. Most organizations identify all systems and software in need of backup as part of their overall technical plan. This plan will include how and when they are to be backed up. Even individual computers may need a backup via a network to a specified hard drive, CD/DVD, external network, or designated cloud.

Backups may be done in real time or continuous. Usually, the organization will set the priority for critical systems and then secure off-site storage (in a format as determined). Data that changes frequently may be backed up daily, such as MLS and customer information. Large and/or heavily used data may be replicated to another physical location in real-time to assure continued access in the event of a problem or disaster.

Redundant systems may seem complex and expensive, but they are usually part of most MLS vendor-supplied services. A systems administrator may be responsible for the process, which is nearly invisible to any individual end user.

Backup Best Practices

Step 1. Identify all systems and data backup.

Step 2. Back up all systems and data on a schedule.

Step 3. Test backups to ensure recovery and restoration.

Recovery matters, which is why the exercise of backing up critical and non-critical systems should be considered incomplete without the testing of those systems. Best practices suggest that organizations confirm the ability to restore any lost data or software.

The testing can be done periodically to ensure that what is backed up is what was expected to be backed up, that data and/or software must be restored to full use, and that daily operations can be resumed with little or no data loss within a reasonable timeframe. While risk tolerance may allow financial reports to be delayed by hours or days due to system problems, customers should be able to access services within minutes after any issue or emergency.

One solution to help achieve these goals is to back up some systems and software to a cloud-based service. This allows for an organization to forgo buying and building infrastructure and still support computing activities such as data storage and software usage. Instead, it shares partner-provided resources and services at a cost savings. Most organizations evaluate the costs and benefits of such cloud solutions to determine the best back-up strategies available.

Data Breaches

If an organization experiences a data breach, it is usually in those systems that are used by their customers. The most common reason for data breaches are customers who attempt to misuse a service feature for personal gain or a business advantage. The second most common reason for a data breach are business partners who may repurpose data for unauthorized uses or distribution.

Either way, such breaches of customer or consumer data are unlawful and can be damaging to business reputations. Since they are usually considered an infraction of contractual or membership obligations, they can be mitigated as such.

Occasionally, data breaches may occur when an organization experiences a malicious or curious attack on its networks or systems. Usually, these attackers seek to acquire data and software or damage and disable software or systems. Preventive measures should repel these intrusions and protect systems and data. What sometimes makes preventing these attacks difficult is that intruders leave only minimal evidence of their efforts in system logs.

In other cases, system attacks aim to cause a Denial of Service (DoS) error, whereby the attacker attempts to overload a system and prevent authorized access/use or otherwise cause poor system performance. Network managers should inform management, leadership, and legal counsel as appropriate. A course of action needs to be defined in the disaster plan document.

Credit Cards and Personal Information

MLSs and associations usually accept payments for services and membership via credit cards. The payment card industry (PCI) was formed by card issuers to set data security standards for the acceptance and processing of payments. This set of standards imposes requirements on nearly every business that accepts electronic commerce. Business partners that provide payment systems may meet many of the requirements of the standards for an organization.

Those partners should confirm in writing that they comply and if there are any further steps that may be required by the organization. Even with partners, the organization still retains responsibility for the secure storage and management of any personal information that may reside in its customer files (physical and electronic).

Organizations should expect audits that will be periodically conducted by the PCI to ensure that the internal procedures are secure, the software in use for processing payments complies, and all personal and financial data is segregated and secure. For example, a customer management system that does automated billing must also meet data security standards requirements.

All efforts to share responsibility for financial data security and prevent cyber crime place additional technical and procedural burdens and awareness on the organization. While there are three steps for adhering to PCI data security standards, these steps should be looked at as a continuous, ongoing process rather a singular event.

PCI Data Security Standards

Step 1. Evaluate. Inventory IT assets and credit card processes, and analyze them for vulnerabilities that expose cardholder data.

Step 2. Remediate. Fix vulnerabilities and do not store cardholder data unless absolutely necessary.

Step 3. Report. Submit compliance reports to acquiring bank and card brands with any required remediation validation records.

Security systems should be employed to protect the physical and intellectual property of the organization.

- Such systems must be monitored and tested regularly.
- Certain systems may require segregation and require specific procedures.
- Activity and usage of systems and networks should be monitored and examined.
- Any attacks or threats to networks and systems require quick resolutions.
- Firewalls and antivirus software should be employed across all systems.
- Software should be regularly maintained and updated for services and security.
- Backups of all critical and non-critical data and software should be scheduled.
- Scheduled backups of all systems and services should be frequently tested.
- Credit card and financial data must meet specific policies and procedures.

As an emerging trend in many markets and with new home performance indicators that may not be recognized, early adopters among MLSs have experienced agent avoidance on the front end. Compliance procedures help alleviate avoidance by proactively monitoring and providing support to those agents, encouraging adoption.

Big Data | Small Data

Much of the MLS business is based on the aggregation, management, and presentation of data. The data is acquired from many sources — public and private — and presented through various software tools that support customer interests and requirements. The management of these vast amounts of data can be accomplished internally or externally with some combination of systems, software and staff support.

The organization is ultimately responsible to meet customer expectations through a variety of tailored products and services as determined by the organization's business plan. The real estate data ecosystem in which the organization operates consists of data providers (e.g., MLS, their vendors, etc.), data consumers (e.g., brokers, third-party vendors, etc.), a standards body that defines how data should be structured and transported (RESO), and an industry trade organization that provides best practice guidance (CMLS).

Data Policies and Distribution. Most MLSs and associations present an array of data services that include a set of core services and various optional services. For example, an MLS may provide access to its data via a vendor-supplied interface or in-house system with similar features.

It will usually provide access to various portions of its available data. This data is subject to the restrictions, policies, and user agreements or licenses for specific use.

An MLS or association is also responsible for monitoring where the data are distributed and how they are used. This enforcement of contract and license terms is challenging as some recipients are willing to bend rules or terms for their personal or business needs. Periodic reviews of the consumers and destinations for MLS data may reveal misuse.

Each organization needs to determine what resources must be applied to monitor data distribution, how to resolve a given situation, and what level of enforcement or sanction is appropriate. Leadership, management and legal counsel all need to review rules and policies and what procedures should be followed to correct or stop misuse or abuse. Organizations may check vendors as well. Some vendors have solutions that can help.

	Ensure data provided complies with RESO standards: Data Dictionary and RESO Web API certification.
	Comply with the NAR IDX and VOW policies: MLS organizations owned and operated by associations of REALTORS® are required to adopt and implement the RESO Standards, including: the RESO Data Dictionary, the RESO Web API and they must keep current by implementing new releases of RESO Standards within one year from ratification. (See NAR Policy Statement 7.58)
	Ensure brokerages can access and retrieve their content as allowed by the local MLS rules, regulations, and applicable laws. Where allowed, content can include listings (off-market, in progress, coming soon), media, agent/office rosters, open houses, agent tours, saved searches, customer contact data, etc.
	Ensure all data consumers are aware of the RESO certified resources available.
	Provide clear documentation outlining all available resources.
	Ensure each resource has a record modification date specific to the data available in the resource; such as an image modification date indicating when the image was last updated.
	Provide the version of compliance for the server, data dictionary, and API.
	Provide clear documentation outlining permitted use, as well as restrictions on use, of data provided.
	Monitor data consumption and API usage to ensure data consumers use efficient data and media selects.
	Content deleted from the host server (listings, media, saved searches, etc.) are clearly identified for data consumers so they can remove their copy of the stored data.
	Provide a minimum of four weeks' written notice to data consumers prior to making significant data changes, which may include database schema changes (e.g., new fields, deleted fields, field name changes, field length changes, data type changes, etc.).
	Provide access to a test platform (staging server) to data consumers for significant data changes at least two weeks prior to release. Vendors many require additional charges for this option.
	Ensure system availability exceeding 99.9 percent with acceptable performance from API requests. SLA may require additional expenses from your provider for support.
	Provide an in-house or vendor contact information (preferably a group email address) to data consumers for assistance with access. Reply promptly to requests.
	Recommend data consumers and service vendors be RESO members and participate in the standards creation and refinement process.
	Recommend data consumers and service vendors certify their client(s).
	Requests for IDX feeds/downloads must be acted on by the MLS within five business days from receipt, barring extenuating circumstances related to an individual's qualification for MLS participation, and review of the participant's and vendor's use of the IDX information consistent with the MLS rules, in which case an estimated time of approval or denial must be issued.
	MLSs must, if requested by a participant, promptly provide basic downloading of all active listings, a minimum of three years sold listing data, non-confidential pending sale listing data, and other listings authorized under applicable MLS rules, and may not exclude any listings from the information that can be downloaded or displayed under IDX except those listings for which a participant has withheld consent, or listings for which the seller has prohibited Internet display.
	Request/require data consumers change their access passwords/passphrases at least annually. This will assist with data security as well as maintaining current data consumer contacts.
	Require data consumers secure all credentials and data stored.

Data Services and Data Consumers. Common data services include IDX, VOWs, and syndication. Internet Data Exchange (IDX) allows the member to publish this data on their public-facing website or app.

Virtual Office Websites (VOWs) allow the publication of data to consumers — subject to a brokerage relationship with the specific consumer — as defined by law and policy. IDX and VOW data services are also subject to local and sometimes national policies and guidelines as approved by the organization's board of directors. They should also be subject to agreements that define the rules, policies, and permitted use of the data.

Syndication is the distribution and publication of a member's data on various public websites and apps as specified by the member. Syndication can be accomplished by directly providing data to a provider or through a syndicator who redistributes data from a data feed.

Other data feed types are designed for an organization and their unique goals and use cases. Examples include data sharing arrangements through software vendors or other networks, publication of limited information about market activity and sales in area newspapers, and custom defined data sets for uses such as government activities and academic analysis. This data can be customized in various ways.

Data may be retained in either a persistent or transient manner. Persistent retention simply means the data is replicated (copied) elsewhere. Transient use means that only the specific, selected data is retrieved for display at the time of request (e.g., in "real time"); it is selected and displayed — perhaps even temporarily cached — but not necessarily copied and saved for reuse. Both use cases have their advantages and disadvantages.

Storing the data can be costly but may be required based on the type of actions to be performed on the data, or to support a certain service level agreement (SLA). Using the data in real time isn't ideal for searching large amounts of data at once, or calculating statistics on the fly for instance, and may require additional fees from the API vendor for hardware to support large-scale queries. In short, both use cases have their place based the requirements of the data consumer, and as supported and approved by the data provider.

There are a number of additional best practices, sourced from industry experts, regarding the consumption and publication of data. In cases where applicable, an organization may benefit from applying these best practices to their operations.

	Know the RESO certifications that the data provider has achieved and utilize the certified resources and data feeds.
	Ensure data pulls from the API(s) are as efficient as possible. Utilize the specific resource modification date available when replicating data to a local server. Incorrectly accessing MLS data through API(s) like the Web API or RETS can cause unintended consequences, such as a degradation in overall performance of the MLS Data Distribution System or increased MLS costs in resources such as bandwidth.
	When available, pull the payload specific to the data use case. For example, pull the IDX payload if only IDX data is desired.
	Comply with the MLS data access and display licenses and rules and regulations.
	Maintain an up-to-date copy of the data provider's metadata for reference and troubleshooting. Consuming applications and services should be "metadata aware" whenever possible. This means it is able to react dynamically to changes in metadata to prevent failures resulting from a change in metadata.
	MLS's IDX download must be refreshed to accurately reflect all updates and status changes no less frequently than every 12 hours or sooner as required by local MLS rule or policy.
	Join RESO and participate in the work groups. As a data consumer, your experiences and expertise will assist with the creation and improvement of the RESO standards.
	Ensure all content locally stored is secured using industry approved standards.
	MLS organizations owned and operated by associations of REALTORS® must comply with the NAR IDX Policy. Leverage the policy and RESO staff for assistance with enforcement of the policy when brokers are unable to gain access to data as required under the policy.
	Provide a group email address to data providers to ensure contact is maintained regardless of role or staff changes.
	For auditing purposes, the vendors consuming RETS (or API) data should track and provide a list of their customers and the datasets they consume and manage on the MLS' client's behalf. This information should be provided to the MLS quarterly, at a minimum.
	Provide access to a test platform (staging server) to data consumers for significant data changes at least two weeks prior to release. Vendors many require additional charges for this option.

APIs, RESO, and the Data Dictionary. APIs (Application Programming Interface) generally provide access to tools and resources, such as data, which developers can use to power their applications. API and data standards are defined and supported by the RESO. Many MLSs, associations, and business partners are members of the not-for-profit organization.

RESO relies on member participation in the definition of standards and includes agent, broker, technology provider, and MLS perspectives on the standards it defines and supports. RESO members meet many times per year to discuss industry changes and standards evolution. Its efforts help ensure data accuracy and interoperability, increasing value to data consumers.

Standards remove ambiguity and diminish incompatibility. In short, standards make it easier for programmers to handle real estate information from many different entities as it forces consistency when exchanging data between different systems.

The Real Estate Transaction Standard (RETS) is an API designed mainly for the replication (or persistent) use case outlined above. It has been in widespread use for more than a decade. And while a modern replacement called the “WebAPI” is rapidly being adopted, RETS continues to be heavily used.

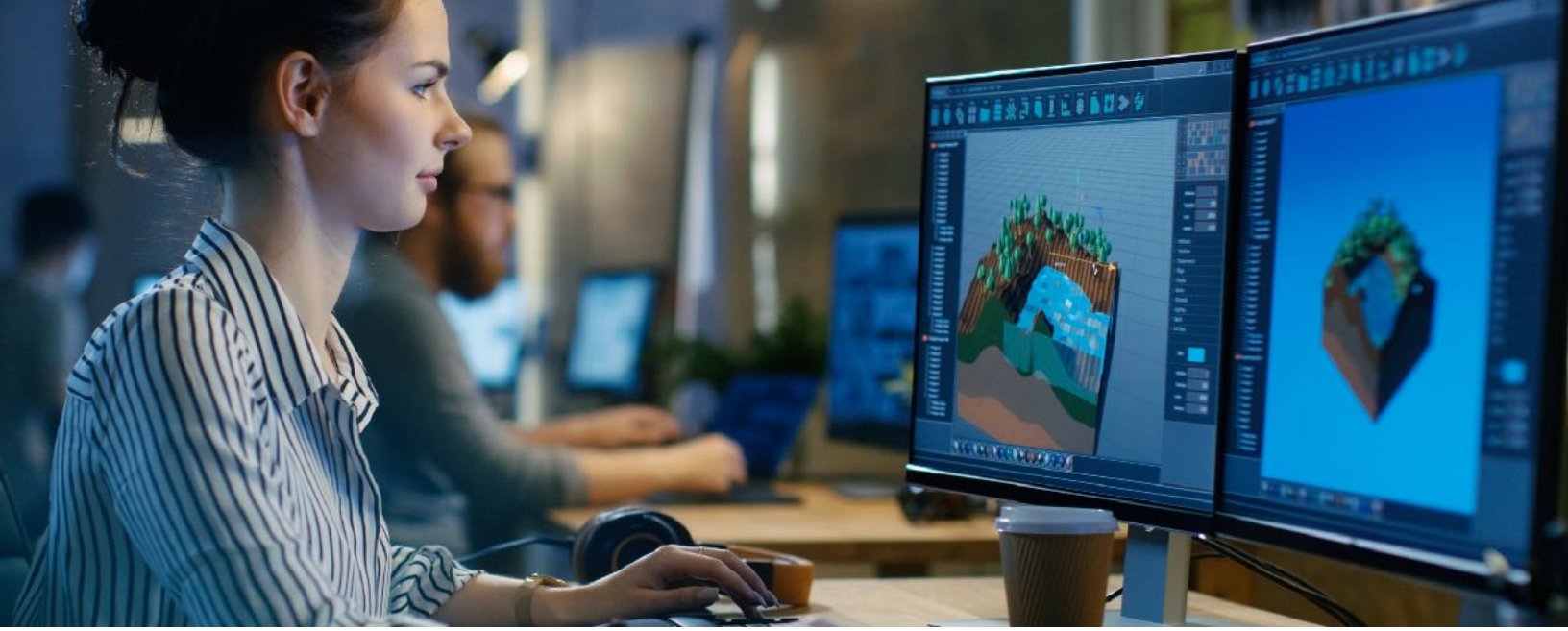
The RETS work group within RESO has been discontinued and no new changes or improvements to this standard are planned. The transport work group within RESO is focusing all efforts on the evolution of the WebAPI.

The WebAPI is the next generation real estate API and is generally intended for real time (or transient) use. This relatively new standard is based on OData, which is an open standard that should allow new entrants and established vendors to develop applications and services more rapidly and easily. OData is a globally recognized technology standard in wide use outside of real estate.

Replication and real time use are not prohibited by either standard, and the choice of how to employ either API is completely up to the data consumer and data provider, in terms of their needs and what is allowed and supported under the data provider’s license agreement and terms of use.

The Data Dictionary provides a common data format for various real estate data resources (e.g., property, member, office, etc.). This format is intended to ensure interoperability for vendors and other data consumers working with multiple MLS partners. This common format defines specific field names, data types, field lengths, and lookup lists (enumerations) so data consumers know what to expect when working with each MLS.

Creating a routine that imports or accesses data from multiple sources, all in the same format and that “speaks the same language,” is hugely efficient for the industry and it supports rapid innovation. In the past, proprietary data formats meant creating custom routines for every data set from every MLS. The Data Dictionary solves this pain point and will continue to evolve as industry needs change.



SOFTWARE SYSTEMS

There are business functions that rely on software: word processing, presentation creation, accounting, human resources, networking, software as a service (SAAS), and operating systems. Each require different degrees of support and monitoring.

Different software packages reside on different operating systems, including Microsoft Windows, UNIX, Linux, iOS, and other proprietary or open source platforms. All of them will have benefits and shortcomings related to compatibility, support services, bug fixes, and cost.

The organization should evaluate what systems best meet the needs identified in its technology plan and through its ongoing business operations. MS Office has become a standard software application as it is easy to use and in common use. There are similar applications provided for an Apple Mac environment. MLSs and associations need to maintain several key enterprise systems as part of their business and services too.

Sometimes a consultant may be retained to assist with the development of a review process and recommend available software products before a major system being purchased and deployed. Organizations may put out an RFP to identify and invite qualified providers to present their software solutions.

The RFP will define the product specifications and the type of consultation being sought by the organization. It will detail the format of an acceptable response and the timelines under which the organization is working. These parameters are essential to the evaluation process, which will often involve leadership. The evaluation will create a framework of comparison of features, references, and finances that will lead to discussion and a decision for purchase or license. Some staff members or departments may also have specialized needs that should be included for within the plan.

Software Best Practices

Practice 1. Software should increase productivity, security, and accountability.

Practice 2. Program licenses must be maintained for all software as required by providers.

Practice 3. Upgrades to software will be applied as necessary and included within the budget.

Practice 3. Consultants can assist with identification and evaluation of software.

Considerations in selecting software may include: cost of software (up front and ongoing), satisfaction of other organizations that use the products, the ability to transfer existing data into the new system, and the learning curve for effectively using the new software in the organization's business.

There may be a substantial impact on staff with the introduction of new association management or CRM software and on customers with the introduction of new MLS software. These situations will require a comprehensive plan for implementation.

The plan should identify whether the implementation is internal or external and include information about the decision process, timetable for launch, expected training and adoption rates, and contingencies. Any plan should provide for not only training, but also follow-up support that will ensure the software is properly used.

As adoption takes place, the purchase review process measures whether the software meets expectations and the current needs of the organization. This should also provide room to grow as the business evolves.

Software is usually considered intellectual property and subject to licenses or other agreements. Even shareware and open source applications have some limitations on use, reuse, or alteration. Management should ensure appropriate licenses exist for all software used in the business in coordination with legal counsel.

There are many resources available within the industry to advise and assist organizations. One such resource is the The Center for REALTOR® Technology (CRT), which is a center of the National Association of REALTORS®. CRTLabs offers open source solutions and applications that address a number of industry challenges. Its staff is noted for responding to questions, offering guidance, and providing referrals.

MLS Software

MLS software systems are at the core of most organizations. This system evolved from the computerized index found in the front (or back) of the formerly ubiquitous “Active Book.” What began as the simple “search and print” phase has become a robust “analyze and present” software model.

The current iterations of MLS software systems provide a wide range of features that allow customers to manage their real estate information, access a variety of related databases, maintain contact with clients and customers, present analyses, and provide consumer presentations.

Issues such as bandwidth, storage space, and computing power no longer limit the quantity of data that can be stored, the locations from which the services can be accessed, or the sophistication of the materials and reports that can be created and shared.

Organizations have several industry suppliers that provide competitive MLS software systems. The selection process is a detailed procedure that involves money, personal preference, organizational politics, and technological suitability. In most cases, regardless of the vendor chosen, they will provide continuous improvements to their software as it evolves from user input and competition.

MLS systems today are generally web-based solutions with vendor-hosted servers in secure locations. There are some larger organizations that create and manage their own in-house systems with development and programming staff, but the cost of entry and complexity of operations are cost prohibitive for most organizations. Most recognize that software development and support is an art in itself and a competency outside those of the general MLS or association.

Common features of MLS software include the ability to manage listing content, search data, create presentations and reports, maintain client and customer information, and keep in touch with customers via email or web portals, present maps and photos, manage documents and photos, and integrate related data from many sources. It also includes mobile apps (native apps, mobile aware, and mobile responsive websites) that give the additional ability of using GPS location technology.

Although mobile apps have limitations and are generally not as robust as their desktop counterparts, they do offer data access for the user to be productive out in the field.

Infrastructure Software

Association Management and Customer Relationship Management. Customer relationship management (CRM) and association management software contain personal and business information about customers and their services, purchases, involvement, and other activities. There are several commercial systems offered as standalone products or as part of an MLS software system.

Regardless, almost all integrate the varied activities of the customer as well as those of the organization. Some other methods of system integration are organization websites, state and national organization National REALTORS® Database System (NRDS), or other systems such as lock boxes, financial systems, and payment systems. CRM applications also vary in complexity and the ability to customize for local needs.

Accounting. Few companies can operate today with their finances managed solely with paper ledgers and a checkbook. Financial accounting software varies greatly in complexity and features but. in general. provides for the functionality and reporting capability required by financial best practices. The software will be able to generate receivable accounts based on customer activity, MLS systems, or other subscription services; provide general accounting for the organization's assets and liabilities; create sufficient standards; and ad hoc reports to meet internal or regulatory reporting requirements.

The selection of accounting software should be done in coordination with finance staff. Accounting systems should be operated in a secure manner to ensure that only employees requiring access to the software can do so, much as the company checkbook is kept in a locked drawer or cabinet. CMLS Financial Best Practices provides more information on this topic.

Contract Management. Most organizations manage many and diverse contracts, licenses and agreements for participation and services. These documents have a lifecycle from agreement through fulfillment to renewal. Software can expedite this process by providing management of terms and dates, alerts for agreed-to changes or price increases, records of modifications and inclusion of electronic signatures. The benefits of these features include management of the exceptions or subsequent events and financial and analytical tools as well as the reduction of paper files and records. See CMLS Legal Best Practices for more information.

Help Desk/Call Centers. Customer support is a key activity of most organizations and may be conducted by staff or outsourced to competent vendors that will tailor the support to the needs of the organization. The software that supports this activity varies in complexity depending on the size of the organization, the volume of calls and inquiries, and management's requirement for system activity information and reports. The implementation of help desk software or applications should be specified by and coordinated with the training and support staff.

A simple help desk application may allow staff to access a customer's business information when receiving a call and then annotate those records to reflect the content of the inquiry and any resolution or outcome. Staff can identify that callers have a repeated issue or that the issues are external to those systems operated by the organization. These entries may contribute to a knowledge base of issues and resolutions that can be referred to by staff or perhaps customers, providing yet another support resource.

Help Desk Best Practices

Practice 1. Customer support and help desk operations require appropriate software.

Practice 2. Communications and online applications will be available to support business operations.

Practice 3. Evaluations of the services provided are ongoing and include surveys, performance metrics, and observations.

Sophisticated systems are usually integrated with telephone systems (VoIP) to manage incoming calls, track wait times, and review other statistics of interest. They may provide some degree of voice response, requesting the caller to broadly identify their issue by voice or keypad, and directing the caller to a resolution more quickly. Help desk add-ons might include use of software that allows staff to view live what the customer sees (screen share), providing a higher level of interaction and support.

The selection and deployment of a sophisticated help line or call center is a fairly complex project. If outsourced, it requires identification of the organization's requirements and a separate request for proposals (RFP) process. Potential service providers must be vetted and a contract carefully negotiated. Following the installation and introduction, the system must be monitored for activity and performance. If hosted in house, staff must be trained to operate and maintain the high quality of response and aid as expected by customers on whatever software and telephone systems are selected by management.

Office Productivity Suites. Many organizations are most familiar with the Windows Microsoft Office suite of products that provide word processing, spreadsheet, database, presentation software, Office365, or SAAS. These products integrate with each other and allow individual productivity as well as collaborative efforts. Similar solutions exist for Mac OSx and Unix environments. The software can be licensed for individual users or for the enterprise and software suites can be extended to include web development and maintenance as well as design and publication.

Product Management and Support. Software must be managed. Large systems require periodic updates, frequent patches, fixes for bugs and programming changes. These may be tracked internally by the software (e.g., Microsoft Service Packs or MLS software vendor) or may require the organization to track patches and fixes made by the internal staff. All such fixes must be tracked and managed, either through simple record keeping or more sophisticated software.

Web-based Services. Most organizations utilize many web-based software services and applications. Net Meetings and voice over Internet protocols (VoIP) such as Skype are two examples. Each provides an application to conduct business virtually, removing the need to meet face to face. A schedule can be set, notices sent by email with the appropriate login/dial-in codes, and a meeting conducted. This includes the capacities for video (participants being able to see each other), sharing of documents, and the exchange of both voice and text information during the meeting.

Training and customer service may employ webinars and video in their support efforts. Webinars can be conducted using voice, prepared images, and live video to present specific topics or general information. Benefits include the convenience of flexible timing (available on demand), the ability to vary and specify content (i.e., short bytes), and self-selection of the audience and interest. Software and services are available to the organization to support these efforts or to produce them in house.

While fax machines still exist in most offices as stand alone devices or as part of a multi-function printer/scanner, many faxes are now generated by software and sent/received via the Internet. Email has replaced the need to fax many documents as they can be sent as attachments rather than a paper-to-paper transaction. Some organizations manage their high volume document systems by allowing customers to fax an original document with a uniquely coded cover sheet to an internal system that converts the document to a PDF file. The system then assigns the PDF file to the appropriate place in the organization's systems and data files.

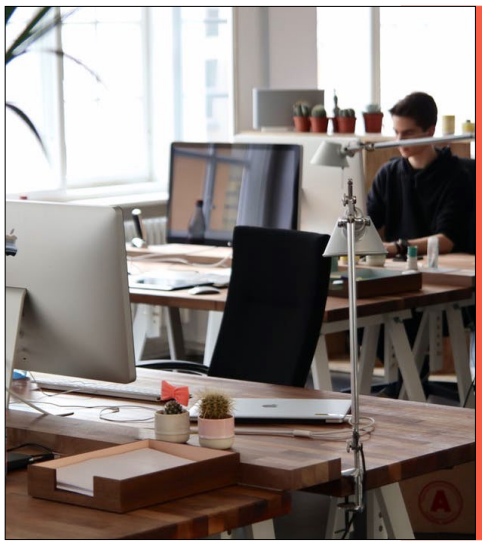
Emails are a preferred method of communication. They allow information to be sent to a broad or specified audience, or specific information to be sent to a select recipient. Many software applications will provide a merge function to combine the communication with a mailing list of email addresses and automatically send the communication.

Some software applications provide detailed information about the delivery and receipt process — how many were delivered, bounced, or opened. This includes newsletters, calls to action, and system changes. Occasionally an organization will outsource some electronic communication activities to a business partner that will provide all of the services and accountability.

Software Development

Notwithstanding the complexity of developing MLS software systems, most organizations will have internal resources or external partners that will provide some degree of programming support and project management.

Websites can be considered one example. Website development, programming, and content development is often done with some mix of internal and external services. In some cases, a business partner may develop a website template and then provide some training to internal staff members, allowing them to update content or modify the layout on a regular basis.



Software Development Best Practices

Practice 1. Customer support and help desk operations require appropriate software.

Practice 2. Communications and online applications will be available to support business operations.

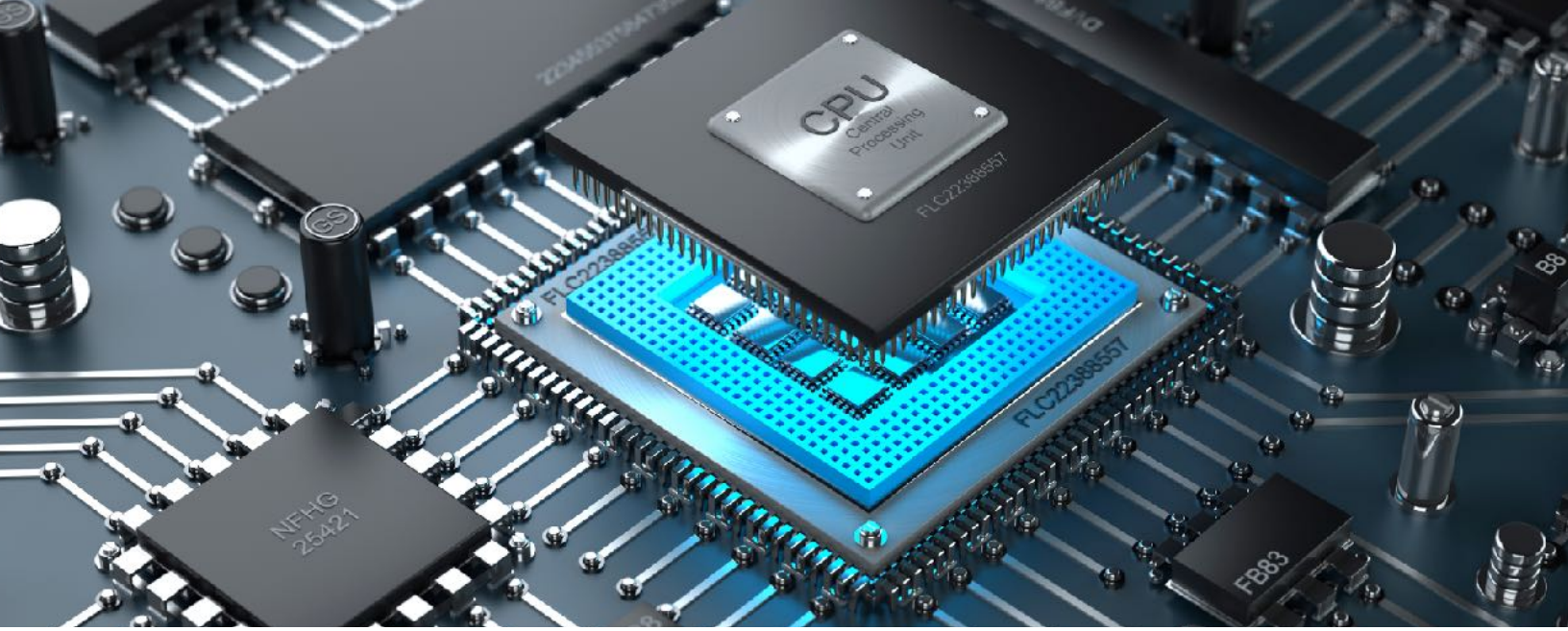
Practice 3. Evaluations of the services provided are ongoing and include surveys, performance metrics, and observations.

The specification, programming and testing of software should not be underestimated. It requires talent, time, and a significant capital investment. While enthusiasm and the desire for independence from vendors may seem like worthwhile objectives, many organizations learn that those two reasons are not sufficient alone.

The competencies to develop software are usually separate from the core business activities of an organization and require substantial management and oversight. Project management is an art that not only holds the vision in sight, but also ensures that schedules are met, programming is adequately documented, and resources (human and financial) are available and properly applied. See the CMLS Technology Section Council White Paper: A Case Study In Project Management.

Software Testing. The evaluation of software is an activity common among all organizations. The purchase or licensing of new systems such as accounting, MLS software, and CRM services are regularly reviewed for available features, costs, conversions, responsiveness, and overall expectations.

Testing is often a staff and customer responsibility. In the case of an MLS system, it may be advisable to involve key customers in testing software functionality and usability prior to a general release. This can ensure the validity of the data as well as increase the adoption by the customer base to ensure success.



HARDWARE SYSTEMS

Technology has rapidly changed in the past 30 years and continues to do so at an increasingly fast pace. Whereas big computers and equipment were once locked behind closed doors and plate glass windows, the same amount of computing power can be found on individual smart phones, tablets, laptops, and desktops.

Where once it was sufficient to only know enough, now it is incumbent on staff and customers to be tech savvy, learning new skills on a regular basis. This also requires the organization to provide the financial and physical resources to maintain these technical tools and technical skills required in order to remain productive and competitive. This not only applies to employees who need to drive business activities, but also the support services used by customers.

Computers

There are a wide variety of devices that provide computing power. Unless outsourced, the organization needs to manage all of these devices as physical assets and business tools, keeping track of the asset value, location, quality, and age of the operating systems (as well as any software that resides on these devices). Computers and other devices must be regularly replaced before they age to the point of likely failures. A standard rate of replacement is every three to four years, provided they are maintained with periodic backups, updates, and maintenance.

Peripheral Devices

Most organizations provide a wide variety of devices for the input, output, and storage of data and information. Regardless of the device, most have become more

compact, readily accessible to several operating systems, and capable of connecting to other hardware via a Wi-Fi network. Printers, for example, have become more versatile as scanners, fax machines, and copy machines. Whereas some scanners remain independent, primarily used to convert paper documents (receipts, invoices, graphics, etc.) into high resolution or large format electronic documents (.pdf or .jpg).

There are many other devices to consider. Copy machines, for example, now offer features that were previously only available through staff effort or a print shop. They make specific copies, print on various sized papers, and allow for two-sided printing. They can insert a cover or backing, collate pages, and bind paper to produce a finished report. Most connect through a network that is accessible to staff via individual computers. Some fax or email scanned documents to the specified recipients. (Always check for and destroy stored copies when disposing of decommissioned copiers or printers.)

While becoming less common, modems still exist. Some are used specifically for credit card readers or banking systems that process checks or credit cards.

Storage devices vary in size and function, with some models storing terabytes of information. Web and software servers can also provide a similar function (cloud storage), creating redundancies that replicate and protect data. Some organizations also outsource data centers to store, backup, and monitor information as well. External DVDs are being replaced by USB thumb drives that are smaller than a pack of gum. In fact, more and more notebooks, laptops, and desktops exclude an internal DVD drive (although external DVD drives may be connected) whereas USB thumb drives store more data than DVDs and sometimes have security features.

In addition, some peripherals are built in to existing devices. Most devices, for example, are equipped with a camera and microphone. While external cameras and microphones may be employed for specific reasons (such as high-quality or stand-alone productions), many devices produce professional audio and visual recordings.

Hardware Best Practices

	Computers should be maintained for capacity, connectivity, productivity, security, and compatibility.
	Equipment should meet the production requirements of the organization as defined in a plan.
	Devices may extend beyond traditional desktops to include phones, tablets, and storage devices.
	Networks must provide security, reliability, redundancy, and adequate bandwidth.
	Investments must be made to keep all systems current, often about every three to four years.
	Critical systems require additional attention in terms of performance and maintenance.
	Networks must be designed to provide security and connectivity for both data and communication.
	Storage devices and built-in peripherals may require additional organizational policies.
	All data centers require active monitoring to ensure competency, security, and risk tolerances.

Data Centers

Many organizations rely on their business partners to host and support critical or specialized business systems. The business partners will provide a secure data center with adequate capacity for computing power, data storage, network communications, and security. It will also provide the necessary electric power, floor space, and access as required or agreed to.

It is usually irrelevant where the data center is located athough most have been built only after great evaluation, planning, and construction. In most cases, so have any web or other network connections. These too must meet the organization's needs.

Some organizations choose to host their own data center in a secure location of their choice and assume the responsibilities connected with such an operation. Most organizations take a hybrid approach, preferring to host critical systems externally and all other systems internally. Some enlist additional business partners as well.

Most data centers will provide reliability and redundancy that meets or exceeds the needs of the organization. While it was once acceptable that customer services may go offline from time to time, today's customers expect uninterrupted services — help desks are often the first to be overloaded with calls when systems fail. This is also why sufficient bandwidth to support the actual and peak traffic is required, as are adequate web servers and data storage.

Redundancy of all these system is required should a primary path or critical device failure occur or become unavailable. Many data centers operate a secondary center to which traffic can be redirected in the event of a failure or disaster. The fail-over to the secondary center is usually transparent to the customer or end user.

For these reasons, choosing or building a data center is a complex undertaking. Adequate facilities are available in most locales, but some organizations look for national data centers with substantial bandwidth and power, and minimal natural risks such as earthquakes, storms, flooding, etc. Organizations should always carefully evaluate their needs, risk tolerance, and competency in their selection.

Communications

Today, all aspects of technology rely on connectivity: people, software, and hardware. Communications are critical to the organization because they assure the flow of data

and information within the business, between the business and customers, and among the various systems and devices in use every day. Systems specific to communication includes the telephone system, the network connecting office systems, and Internet (and Wi-Fi) access.

Most organizations will operate multiple networks to connect various systems, to isolate critical systems, and to provide greater security across all technologies. The example below shows local computers operating in separate networks and the addition of a VoIP telephone system.

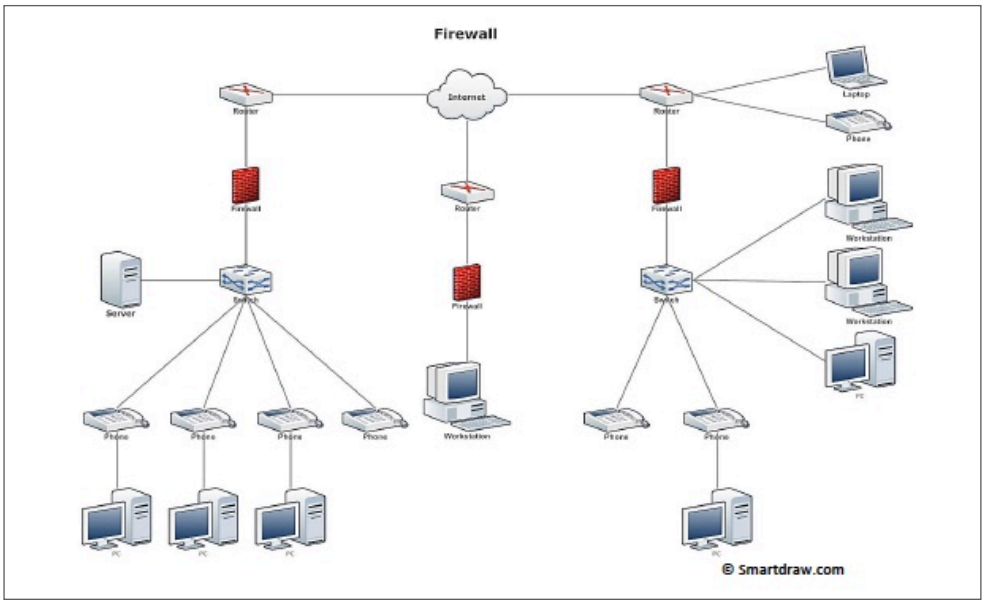


Figure 1: Each organization should draft and maintain a diagram of its assets and their network connections.

Routers are physical devices that identify the network using an Internet Protocol (IP) address, forward data packets through neighboring networks to their final destination (and through their software), and provide the access rights and security for both incoming and outgoing traffic. Most organizations include a Wi-Fi network to further expand connectivity.

This requires a Wi-Fi router that is properly configured for general use or secured use. Organizations may provide a Wi-Fi network onsite for the convenience of their customers or for specific situations such as a training or support center. Some customers may bring their own devices (BYOD) that can then quickly be connected once these visitors have been given a password.

Organizations that utilize Wi-Fi for all connectivity rather than physical cables need to take additional steps and establish procedures to ensure the security and performance of the system. Network Access Control (NAC) devices should be employed to ensure devices that attempt to access the Wi-Fi are authorized and meet the required security profile.

Telephone systems also require hardware and networks. The technical responsibility may be to select and support both. Hardware and network providers can be identified and evaluated through the Request for Proposals (RFP) process or in tandem with other technology decisions.

Some organizations choose to lease their systems and networks. Others prefer to purchase them or outline some lease-purchase mix that makes sense. Determining factors are usually based on the features required, number of devices, and ability of the providers. Other factors such as capability with other systems — such as a help desk or CRM — will also make a difference.

Upgrades and Investments

As discussed, both software and hardware systems require management and maintenance. The most efficient means of planning for management, maintenances and upgrades is to inventory all software and systems. The inventory should include: what it has, where it is located, what its capacities are, life expectancy, and how are they are networked.

Providing this level of detail will allow the organization to better stagger upgrades and new investments. This will provide critical systems and other systems a continuity of operations, with no one system or software solution outpacing the overall operation of the organization.

This approach will provide the organization with a budgetary framework. Critical systems should receive the greatest attention and investment, similar to that of human resources and financial departments. In fact, even those department would struggle without efficient software and systems.

There is practical side to upgrades. It is a function of modern business today and not the product of simply having the “newest and best” hardware as experienced in days past. By balancing the newest technologies with proven functioning systems, and staggering upgrades and investments, many organizations can remain proactive in their approach to business rather than be a slave to antiquated software and systems.

In order to make the best decisions possible, organizations should make it a point to become aware of new technologies and products, especially those introduced through the Council of Multiple Listing Services. In addition, organizations may turn to other industry connections at events and conferences such as RESO, asking peers and other industry leaders.

The organization can also identify products and services with the help of an outside business partner, contracted specifically to evaluate business needs and existing or emerging technologies that may fit within the overall operations and evolution of the organization. Once compiled, an organization can prioritize needs, test solutions, and measure effectiveness versus the cost of the technology.

CONCLUSION

The best way for an MLS to strengthen security, enhance services, and improve overall operations is often central to technical and IT services. This requires organizations to leverage knowledge about individual software, systems, structures, and needs to better understand the real and perceived opportunities and threats facing the organization.

By doing so, the organization will be better able to continually implement timely upgrades and patches in a more efficient and comprehensive manner, quickly add newly released tools and software that can effectively streamline various operations, and ensure business continuity now and in the future. This is especially important for MLSs as a fundamental part of the MLS value proposition to build a better marketplace. This can be accomplished by following the sections outlined herein.

- Establish goals, objectives, and needs
- Audit software, hardware, and systems
- Define internal and external roles and responsibilities
- Improve existing software and system infrastructure
- Test systems for disaster survivability and data recovery

There are several more supplements that can help bring an MLS up to speed on technical issues, including the CMLS Quick Start: MLS Green Field Guide. While these guides can help jump start an initiative, always remember that fields are only the beginning of a successful plan. MLSs must look at the overall business goals.

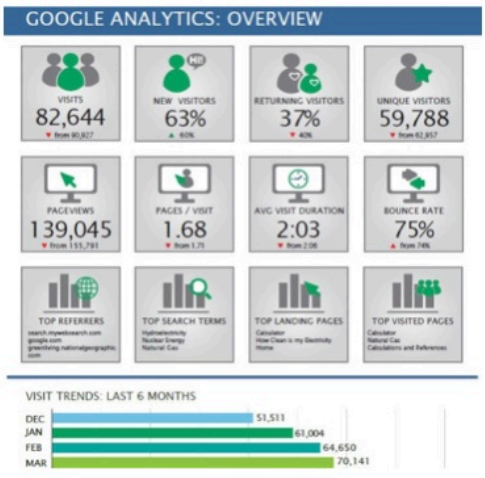
By following these best practices, an MLS is making a conscious effort to step up and become identified as a best-in-class organization. When you accomplish this goal, CMLS will be among the first to recognize your efforts while providing new resources to help move the industry forward.

APPENDIX A
GOOGLE ANALYTICS

Google Analytics lets companies measure advertising return on investment as well as Flash, video, social networking sites, and applications. It provides an abundance of free tools needed to analyze data for organizations of any size, and provides customization, insights, and machine learning all in one place. Visit Google Analytics for more information.

Figure 2: Google Analytics introduces companies to website monitoring and then adds sophistication.

Figures 3 and 4: Google Analytics tracks visits,, engagement, conversions, time on page, time on site, and many other metrics.



APPENDIX B
DISASTER PLANNING

All preparedness programs are built on a foundation of management leadership, staff commitment, and financial support. Without these fundamentals, it will be difficult to build the program, maintain resources, and keep the program up to date.

It is important to invest in a preparedness program in the event of an emergency, disaster, or other business interruption. Consider the following points:

- According to the Insurance Information Institute, up to 40 percent of businesses affected by a natural or human-caused disaster never reopen.
- Customers expect delivery of products or services on time. If there is a significant delay, customers may go to a competitor.
- Larger businesses ask their suppliers about preparedness. They want to be sure that their supply chain is not interrupted. Failure to implement a preparedness program risks losing business to competitors that demonstrate they have a plan.
- Insurance is a partial solution. It does not cover all losses. It will not replace customers. It will not recover data.
- Many disasters — natural or human caused — may overwhelm the resources of even the largest public agencies.
- News travels fast and perception often differs from reality. Businesses need to reach out to customers and other stakeholders quickly.
- An Ad Council survey reported that nearly two-thirds (62 percent) of respondents said they do not have an emergency plan in place for their business.
- According to the Small Business Administration, small businesses:
  - Represent 99.7 percent of all employer firms
  - Employ about half of all private sector employees
  - Have generated 65 percent of net new jobs over the past 17 years
  - Made up 97.5 percent of all identified exporters.

How much should be invested in a preparedness program depends upon many factors. Regulations establish minimum requirements. Beyond these minimums each business needs to determine how much risk it can tolerate.

Since many risks cannot be insured, a preparedness program may be the only means of navigating and mitigating those risks. Some risks can be reduced by investing in loss prevention programs, protection systems, and equipment. An understanding of the likelihood and severity of risk and the costs to reduce risk is needed to make decisions.

Preparedness Policy

A preparedness policy that is consistent with the mission and vision of the business should be written and disseminated by management. The policy should define roles and responsibilities. It should authorize select employees to develop the program and keep it current. The policy should also define the goals and objectives of the program. Typical goals of the preparedness program include:

- Protect the safety of employees, visitors, contractors and others at risk from hazards at the facility. Plan for persons with disabilities and functional needs
- Maintain customer service by minimizing interruptions or disruptions of business operations
- Protect facilities, physical assets and electronic information
- Prevent environmental contamination
- Protect the organization's brand, image and reputation

Program Committees

Key employees should be organized as a program committee that will assist in the development, implementation, and maintenance of the preparedness program. A program coordinator should be appointed to lead the committee and guide the development of the program and communicate essential aspects of the plan to all employees so they can participate in the preparedness effort.

Program Administration

The preparedness program should be reviewed periodically to ensure it meets the current needs of the business. Keep records on file for easy access. When applicable, make note of any laws, regulations, and other requirements that may have changed. For additional preparedness advice, visit Ready, which is a national public service campaign.

APPENDIX C
RESO AND RETS

Real Estate Transaction Standard (RETS) provides an interface for you to easily access data through a RETS-compliant MLS. Vendors that offer compliant utilities allow you the ability to use their services without having to perform double entry and provide the option of easily migrating to new services or systems.

It is important to note that RESO will continue to use “RETS” as a prefix for its original standard product (i.e., RETS version 1.5 through 1.9) but will not do so for future products such as Data Dictionary. Although in use, they are legacy tools.

RETS

RETS provided the original common language spoken by systems that handle real estate information, such as multiple listing services. A common language enables computers to receive information from different real estate systems or MLSs without being specially "trained" to understand the information from each.

Standards like RETS exist in many different fields. Sometimes, the standard simply adopts one of many pre-existing languages that everyone agrees to use. For example, air traffic controllers at international airports all speak English. No matter their native language, pilots are guaranteed they only need to learn one language.

RETS, like many computer standards, was a language that was built for a specific purpose, but the goal is the same: to help programs that deal with real estate information "speak" the same language.

For software developers and providers of services like IDX sites, RETS means having to write programs to use only one language, the common language of RETS, in order to work with many different MLS systems. This means lower costs, products, more competition among vendors, and faster implementation of new systems, all of which directly benefit those who work with real estate information for a living.

RESO

RESO develops standards that are implemented in real estate to make it easier for programmers to handle real estate information from many different entities because standards force consistency when exchanging data between different systems. Visit the RESO Data Dictionary Wiki and RESO Web API for details.

APPENDIX D
SELF-ASSESSMENT

Technical and IT Services	Yes	No	Comments
MANAGEMENT			
Goals and objectives clearly defined in a plan			
Plan identifies critical and non-critical systems			
Internal and external clearly defined			
Adopt a formal written disaster recovery plan			
Test the disaster recovery plan on annual basis			
Staff meets plan requirements and operations			
Outsourced staff/talent meet expectations			
BUDGETS & EXPENDITURES			
Identify income and expenses			
Plan and stagger capital investments			
Inventory internal and external assets			
OPERATIONS			
Staff equipped with required technologies			
Staff properly trained on use of technology			
Activities and processes are documented			
Written policies govern use of technologies			
- For email and networks			
- For hardware and software			
- Checklist for new and departing employees			
Websites are maintained by the organization			
Business-related domains are registered			
Social media is used as appropriate			

Technical and IT Services, 2	Yes	No	Comments
SECURITY			
Facility has proper physical and electronic security			
Security systems and alarms are properly monitored			
Use of passwords and proper policies in place			
- Guidelines available for staff and customers			
- Secondary authentication required			
- SSO available, documented and monitored			
Systems in secure facility, or secured as needed			
- Routers, firewalls and spam/malware installed			
- Systems monitored for availability/performance			
- Staff notified of system issues and failures			
- System reports reviewed for traffic and other quantitative metrics			
Networks are properly configured and maintained			
- Networks are segregated and secure			
- Wi-Fi network security for staff and customers			
Business information is properly secured and stored			
- Credit info and processing is PCI compliant			
- Backups are performed on a written schedule			
- Restoration of systems from a backup tested			
DATA AND INFORMATION			
Policies and legal agreement govern data use/reuse			
RETS and Data Dictionary supported			
IDX, VOW and custom data feeds are available			
Data can be syndicated in general or custom format			
Data access/release is managed by control systems			
API is available for software and developers			
Market and trend reports are produced for customers and management			

Technical and IT Services, 3	Yes	No	Comments
SOFTWARE			
All business operations are met and supported			
- Software is provided to meet job requirements			
- Software versions are kept up to date			
All software is properly inventoried and licensed			
CRM or association management software is used			
- Integrates with MLS, state and national systems			
- Integrates with or provides accounting systems			
HARDWARE			
All business operations are met and supported			
- Hardware is provided to meet job requirements			
- Equipment is properly supplied and maintained			
All hardware is properly inventoried			
Critical systems are backed up and secure			
Equipment no longer needed is disposed of properly			
Data centers meet or exceed business plans and requirements			

APPENDIX E
REFERENCES

Reference List

Apple Inc.
ASAE Center for Association Leadership
Center for REALTOR® Technology
Clareity Consulting (acquired by CoreLogic)
Microsoft
MLS Domains Association (assumed by CMLS)
National Association of REALTORS®
PCI Security Standards Council
Real Estate Standards Organization (RESO)
SmartDraw
Canadian Information Processing Society (CIPS)
salesforce.com
WAV Group

Contributing Organizations

CMLS Techical and IT Section Council
Heartland MLS
Kansas City Regional Association of REALTORS
MLS Listings Inc.
Utah Real Estate

NOTES

published by

Council of Multiple Listing Services
1000 N. Green Valley Parkway #440-583
Henderson, Nevada 89074

cmls.org | 877.505.8805

CMLS

cmls.org