



Records Management: Getting down to the basics

Has it been months, if not years, since you've gone through your old records in the back room full of cabinets or leaning towers of boxes? All too often filing and records management are placed on the "back burner" and can quickly become unmanageable. Here are some tips for where to begin:

Why keep files –The bottom line is, federal law says you must keep certain files and records. Many federal laws are based on PCI compliance, which applies to all organizations and businesses that accept, transmit or store cardholder data, regardless of the size of the organization or the number of transactions. FACTA (Fair and Accurate Credit Transaction Act), HIPAA (Health Insurance Portability and Accountability Act) and Sarbanes-Oxley all need to be taken into account with your records as you or your business can be audited at any time.

What to keep – What you should keep differs from business to business. Consult your legal and accounting staff to determine what your business needs to retain. Consider keeping the following on file: financial statements, past employee personnel records, accident reports, internal audit reports, purchase orders, expired insurance policies, accounts payable and accounts receivable statements, payroll records and summaries. You may also want to consider keeping copyrights, trademarks, patents, audit reports of public accounts, year-end financial statements, property records including blue prints and tax returns indefinitely.

How to keep and secure files – Many companies believe their files are secure but haven't taken into account the impact of a disaster like a flood or fire or the wrong person getting their hands on their files. Files and records should always be backed up. Scan documents to convert them into electronic files and back up your hard drive. Make a hard copy of all files, blueprints and photographs and store the copies off site. Lock all files in a filing cabinet, safe, vault or separate room. Limit access to the files by password-protected computers and selecting only a couple trusted employees with the passwords and keys to your files. If you have a large number of files containing confidential information, consider installing security cameras. Also, consider an off-site storage facility to further secure your records.

How long to keep files – Many people think seven years is the rule of thumb when it comes to cycling out records; however, this is not true for all documents. Once again, talk with a trusted advisor and your legal and accounting staff. Storage lengths are based on federal regulations, so keep in mind PCI compliance, FACTA, HIPAA and Sarbanes-Oxley. Never assume it's better to be safe than sorry when it comes to holding onto documents. During an audit, federal law says they can go through all of your records on hand, regardless of age.

How to discard files – When discarding documents is the right decision, it's critical to discuss the safest and most secure way to properly destroy records. If you are considering using a professional service, make sure you use an NAID (National Association of Information Destruction) AAA approved vendor as it signifies the highest level of excellence of information destruction. Make sure document destruction rules are communicated with staff and roles are clearly defined as to who has permission to handle the destruction of records. Shred files whenever possible, including old discs or CDs with information on them. If you have large quantities of items to shredded, take advantage of local services that offer on-site shredding.

It's also integral to develop a plan for staying organized – Develop a retention and destruction plan that incorporates specifics on document types on file and an exact date each file can be discarded. Also include how you plan to discard of old files, and who is allowed to know passwords and have access to locked files. Commit to updating your retention and destruction plan monthly or at minimum each quarter. Becoming organized may take some time initially, but you will sleep a lot better knowing your most important asset is now protected. 📌



Founded in 1983, A.R.M.S. (Automated Records Management Systems) provides information management and protection services to businesses throughout Wisconsin and Upper Michigan. As a full-service commercial records center, A.R.M.S. provides "Information Management from Inception through Destruction" for customers ranging from small businesses to Fortune 500 firms.