

Why Your Business Needs a Records Retention Policy

What do Sarbanes-Oxley, OSHA, The Family Medical Leave Act, The Equal Pay Act, Title VII of the Civil Rights Act, and any lawsuit that your company is involved in all have in common?

Each has unique records retention requirements that could leave your company subject to fines, legal liability, and potentially criminal prosecution for management. Unless, that is, a corporate records retention policy is implemented and enforced.

Numerous Federal and state statutes have created complex records retention rules that companies are responsible for understanding and implementing. The government mandates this records retention so it can audit compliance with the regulations it puts into place. The Fair Labor Standards Act requires companies to keep and employee's payroll records for three years after the employee has ended employment. OSHA requires companies to keep records of any safety issues or accidents for five years. These are only two examples; companies must keep track of countless other retention requirements. In 2006, Morgan Stanley was fined \$15 million for failing to produce e-mails related to an SEC investigation of analyst practices. Bank of America was fined \$10 million in 2004 for concealing records during a separate SEC investigation related to analyst coverage¹.

Litigation and e-discovery is the other key driver for corporate records retention. The vast volume of documents that are created in a business is all potential evidence in future litigation, making it an important litigation risk management issue. A recent Network World article noted that at any given time, the average U.S. business is involved in over 300 lawsuits². When a company is involved in litigation, organized document retention can be crucial.

Stringent e-discovery requirements were put into place by the Supreme Court in 2006 when it issued new updates to its Federal Rules of Civil Procedure. These rules set clear expectations that a company must be able to produce electronically stored information as evidence within a reasonable time-frame. Many states have mirrored these e-discovery rules in their own set of procedural requirements and those that haven't yet will be following suit soon.³

First, e-discovery can be a time-consuming and expensive process. The e-discovery and document search phase of litigation could cost millions of dollars depending on the volume of information that is requested. A company that is well organized will be able to complete this process quickly and efficiently by having the requested material organized and at its fingertips.

¹ <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/10/AR2006051002046.html>

² <http://www.networkworld.com/supp/2007/ndc3/052107-ediscovery-readiness.html>

³ <http://www.eweek.com/c/a/Data-Storage/Saving-the-Data/>

Second, retaining and finding relevant documents can be the difference between winning and losing a lawsuit. If a company has not retained documents which are important to a case, it may not be able to prove its case and is at risk for a negative verdict. Further, if a requested piece of evidence has been disposed of or destroyed without a clear, uniform, and systematic policy for doing so, a judge or jury can assume that the document contained information detrimental to the case and act accordingly. Morgan Stanley (again!) suffered a \$1.57 billion judgment primarily due to a jury's finding that their document retention practices were insufficient⁴. If records are destroyed as prescribed by a systematic policy, a company can avoid these types of penalties.

A well-implemented document retention policy can help keep a company out of the courtroom in the first place. By educating employees that any document created could be subject to scrutiny in the future, a company can prevent the creation of emails that may be considered offensive, harassing, or that may be misconstrued in any other way. Employees should also be educated about the legal risk of transporting files on thumb drives or transferring data to home computers. These rogue files are hidden risks to your company unless there are appropriate controls in place.

How to get started?

When implementing a document retention policy, a company must first understand the types of records that need to be retained and the appropriate retention period. Document types include employee related documents such as leave requests and payroll records, accounting records such as auditor's reports and invoices, and general business documents such as contracts and business permits. Each state has its own set of rules and there are national statutes in the U.S. and worldwide that have differing requirements. Companies should review each category in light of the applicable laws in its jurisdiction to determine how long that document type should be retained.

The WAND Records Retention Taxonomy is a pre-built structure to jumpstart the process of identifying the major types of documents that need to be retained. It is designed to clearly identify the types of records that a company needs to manage. There are over 350 document categories that can be used to tag documents. A rich set of synonyms have been developed to assist with auto-classification, in case that is a feature your search software supports. It acts as a virtual file structure for organizing all major records categories that must be retained. A company can simply overlay its own records retention schedule to the categories. Or, if a company doesn't have an established schedule, the taxonomy can be used as a catalyst to begin developing one.

Simply, a records retention policy is not optional for businesses today. WAND's record retention taxonomy can help your company develop and maintain a good policy that will minimize your legal risk.

This article is designed to be a high level overview of records retention and is not legal advice.

⁴ <http://www.networkworld.com/supp/2007/ndc3/052107-ediscovery-readiness.html>