Proliferating data coupled with the newly revised U.S. Federal Rules of Civil Procedure rule 37 on spoliation amplifies the importance of a clearly defined and enforced document retention policy (DRP). A DRP equips legal organizations with procedures on a standardized way to review, retain, and destroy documents possessed by or created in the course of business. A well-drafted policy will also identify documents that need to be preserved and maintained, and provide direction on how long to retain certain documents. Furthermore, a prudent DRP that is enforced and followed by employees may be a lifesaver in the event of burdensome litigation.

Reasons for Establishing a Document Retention Policy

A DRP establishes and describes how company employees are expected to manage company electronic and physical data from creation through destruction. There are many reasons why a company should implement a document retention policy. According to Thomson Reuters Practical Law, if a company's litigation hold obligations to preserve documents are triggered by a potential litigation or government investigation, a document retention policy can help it more efficiently determine whether documents from a particular period are still held by the company and find any relevant records. If documents that are relevant to a lawsuit or government investigation were destroyed by the company before it reasonably anticipated the investigation or lawsuit, having a company-wide document retention policy may help demonstrate to a judge or government agency that the company had a legitimate (and neutral) purpose for the document destruction.

On the other hand, intentionally destroying documents relevant to pending litigation - known as the spoliation doctrine - can also severely impair your business’s position in litigation. The National Association of Independent Businesses (NAIB) simply states that “If a litigant requests a document that you cannot provide because it has been destroyed, then a judge or jury may in some circumstances be permitted to conclude that the document contained information detrimental to your position.” They further explain that the primary exception to this rule is if the destruction of the document was reasonable. Evidence of a clear and consistently enforced DRP, enacted for valid purposes, will go a long way to convince the court that the destruction of a document was reasonable.

Benefits of Enforcing a DRP

Crafting and enforcing a precise DRP can yield three primary benefits: efficiency, safety in litigation, and confidence in compliance. Business efficiency is enhanced in a few different ways. Locating key documents quickly when they are needed is a benefit to an enforced DRP. The less time wasted on searching for and locating documents, the more time is spent performing higher quality work. A consistently followed DRP aids as a safety precaution, particularly when litigation seems imminent. Lacking critical documents can have a real affect on the outcome of a case. For example, proving breach of contract will be impossible if you cannot find the contract in question. That is where a DRP can help; it can aid in determining what documents must be retained and for how long they must be stored. Conversely, unnecessarily retaining archives can make a company vulnerable to claims based on old and trivial documents drafted by former employees who may be unable to put their words in the proper context. To feel confident that your firm’s DRP abides by compliance standards, check your state and local laws before constructing. Particularly in regard to document retention, federal and state laws may differ. It is important that you evaluate the nuances in the laws that are applicable to your business and retain the documents for the required period of time.
Developing a Policy

If you already have a DRP in place, keep reading to be confident your policy considers all aspects a DRP should cover. If your firm has not developed a DRP, hopefully this top ten list will offer meaningful guidance. The following list addresses the life cycle elements of the various categories of information (creation, use, maintenance, retention, and disposal, as well as practical tips in developing, planning, and implementing this DRP.

Top 10 Tips for Building a Document Retention Policy

1. Select a point person or create a steering committee.

The chance of developing a DRP without someone who is directly responsible is very low, and even lower for creating a comprehensive plan. Consider appointing a person to manage the process, or better yet, create an oversight or steering committee to lead the work. Compose the team with departmental representatives, including employees from IT and legal.

2. Assess and prioritize the DRP project scope.

At the outset of any project, it is essential to define the scope; by establishing the scope of the DRP and a timeline, the work will seem much more manageable. These tactics will also ease the natural tension between achieving full compliance and keeping the project manageable. Another tip in managing the project while working towards compliance is to roll out retention policies to one data set at a time.

3. Consult with data management and IT personnel.

Assuming that the steering committee includes IT and data management members, this point is for the brave soul navigating a DRP alone. Meeting with IT business partners will be helpful in ensuring that all the different forms documents and data are created, stored, preserved, and backed up at your firm. Consulting with IT professionals will also provide assurance that you are accounting for all forms of electronic data in all devices and media. In the DRP, expressly state that the policy covers all documents and other information in these locations.

4. Pinpoint what electronic and physical documents your business produces, and assign ownership.

It is commonplace for DRPs to begin with listing the policy statement, followed by a retention schedule that lists every possible type of information that the company could have in its possession and the required retention period. This is an important measure to ensure that the DRP explicitly applies to electronically stored information (ESI) and paper documents, in addition to other physical items, such as slides, tapes, and discs. Identify who is responsible for records and determine whether this responsibility should be centralized in a dedicated individual or department, decentralized among representatives of the company's business units, or shared among employees in a records compliance task force.

5. Review state and federal rules.

Address applicable federal, state, and regulatory recrudescent requirements in disposal provisions. For example, the U.S. Securities and Exchange Commission (SEC) requires certain SEC-regulated companies to keep emails for a minimum of three years (17 C.F.R. § 240.17a-4). Determine whether your company's home state has adopted the Uniform Preservation of Private Business Records Act, which includes a definition of "business record." If it does, include the term and definition in your policy; this step will distinguish your DRP from documents that have no retention requirements.

6. Detail instructions on storing, retaining, and preserving data.

Decide how to organize, where to store, how long to retain, and when to back up documents. Describe the method in which to organize and store documents so that they can be retrieved effectively and expeditiously. Describe the categories and types of documents that are confidential or sensitive and cover the steps necessary to protect this type of information. These can include documents containing specific keywords or phrases. Note how often backup tapes may be overwritten, if at all. Categorize documents and specify how long each category should be preserved, and in what format. For example, according to U.S. Securities and Exchange Commission regulations, public companies are required to save audit documents and communications for a minimum of seven years, but states govern how long medical records should be retained. To ensure compliance with regulatory, statutory, contractual, or business requirements, include procedures governing data backup and test the recovery system at planned intervals. For commercial, legal, and operational reasons, set minimum retention periods to lessen the risk of unauthorized access to data. The less data a company holds, the less it has to lose in (for example) a breach and data disclosures.

7. Set guidelines on destroying expired or useless data.

Once a document reaches its expiration for retention, the policy needs to include details on how to handle data. Specify the procedure to dispose of documents once their retention period is up. The routine process of extinguishing expired data will help your
business in managing the ever-growing amount of data. In the event of a foreseeable legal hold, specify how the disposition of
documents shall be suspended under the retention policy when a litigation or investigation is reasonably anticipated.

8. Train employees on the plan and communicate the processes.

A training program for employees on the DRP should not be an afterthought. Training should lead the way in implementing the DRP;
employee training should be available at the time the policy is issued. Plan to answer questions pertaining to a process for special
requests and irregular events (e.g. legal holds). Training and implementing the DRP should be consistent, systematic, and
feasible. At the same time, the policy should be sternly implemented, which can be done by defining penalties for noncompliance.
This may also be the time to identify other individuals responsible for enforcing, monitoring, and updating the policy – share the
duty of DRP enforcement and management.

9. Clearly communicate the employee duty to follow protocol.

Address employee document preservation and disposal protocol clearly and explicitly, and plainly state that employees have no
expectation of personal privacy in either communications they send or receive through the company's email system, or documents
they create or store on company equipment or premises. Prohibit employees from creating documents that are inaccurate,
incorrect, misleading, fraudulent, harassing, profane, racist, sexually explicit, or obscene. Outline the possible consequences for
violating the policy. If not already covered in another policy, such as an acceptable use policy, security policy or Bring Your Own
Device (BYOD) to work policy, it should explain the acceptable use (if any) of the following for conducting company business: home
computers, cloud storage, personal smart phones, personal email accounts, and personal internet sites, blogs, and social media
networks.


As new technologies emerge that intersect with business practices, consider covering new tools in your DRP. Manage risk by using
legal counsel at regular intervals to ensure policies comply with changing regulations and case law.

Conclusion

In the event of an employee resignation whether voluntarily or involuntarily, it may behoove your firm to implement written
procedures for departing employees regarding the return or disposal of company records stored on their personal laptops, universal
serial bus (USB) drives, and personal digital assistants (PDAs). Include instructions for obtaining departing employees’ new contact
details in case the company needs to interview them in the future. The company may also want to analyze the costs and benefits of
using third-party service providers, email archives, cloud retention systems, and software products to implement the
company’s retention practices and disposal mechanisms and incorporate the policy’s relevant requirements into company contracts
and agreements.

The duty of business leaders and managers in the modern Information Age is to establish systems and procedures that will create
efficiencies, safeguard business, and abide by compliance regulations. Yet, a documented DRP alone is ineffective and useless if not
implemented and maintained. Be vigilant of information and data employees are creating, as well as how data are created. Fixing a
keen eye on controlling and managing information will be worth the effort as information continues to expand.

About Thomson Reuters Legal Managed Services

Thomson Reuters has re-envisioned the future of legal process outsourcing services. Legal Managed Services is composed to deliver
results on a global scale. Our best practices approach leverages the right combination of advanced technology, legal expertise and
sophisticated processes to help you accomplish your goals. We will proactively partner with you to create a program that allows you
to expand capacity, improve efficiency and leverage your internal resources more effectively. Turn to us to help handle your most
critical assignments and your most unique challenges of complexity and scale in the areas of ediscovery and document review.

Sources

National Federation of Independent Business, NFIB Guide to Developing a DRP.


The information in this Top Ten should not be construed as legal advice or legal opinion on specific facts and should not be considered
representative of the views of its authors, its sponsors, and/or the ACC. This Top Ten is not intended as a definitive statement on the subject
addressed. Rather, it is intended to serve as a tool providing practical advice and references for the busy in-house practitioner and other readers.