Why You Need a Document Retention Policy

Disposing of both hard and electronic documents in a timely fashion provides many benefits, including reducing labor and storage costs and minimizing the potential that a data breach will expose sensitive information. In addition to routine disposal, the documenting, organizing, and streamlining of how data is stored can also make it easier to quickly find important company information.

In the event of litigation, a document retention policy can lower both the risks and costs of the e-discovery obligations involved. To be effective in this way, your company’s document retention policy must be written, systematically and consistently enforced, and flexible in the event of potential litigation or another circumstance that includes a duty to preserve.

Guidelines for Development

While there are many factors that can impact the creation of a robust document retention policy (e.g., the size of your company, the technology it uses, and the resources that are available), here are some basic steps that can help you put a meaningful document retention policy in place:

- Select a point person or committee;
- Take inventory of your data;
- Review state and federal rules on document retention requirements;
- Create a retention schedule and instructions;
- Set rules on document destruction;

In today’s age of electronic documents, communication, and storage, your company is potentially creating thousands of documents every day.

Therefore, a sound document retention policy for your electronically stored information (ESI) is crucial for many reasons including minimizing costs, reducing litigation, and preventing security risks.
• Note litigation holds and other exceptions;
• Implement document retention training; and
• Review and update the policy as needed.

Select a Point Person or Committee
Appoint one person or a steering committee that consists of department representatives to be directly responsible for the development and implementation of the document retention policy. This is especially important in large organizations.

Consult with or directly include stakeholders such as data management, IT, and legal as the prime movers on the document retention planning team. Without a person or team of people taking accountability for the development and implementation of the document retention policy, it is unlikely to be successful.

Take Stock of Your Company’s Data
Inventory the types of documents (electronic and physical) that your organization produces or handles, as well as all of the different locations where these documents may reside. Types of records or documents might include:

• Project documents (e.g., drawings, change orders, correspondence, and subcontracts);
• Tax documents (e.g., sales tax returns, cancelled checks, and payroll tax returns);
• Personnel information (e.g., personnel files, disability benefits statements, withholding statements, and contracts);
• Insurance documents (e.g., policies, claim files, and accident reports);
• Financial documents (e.g., deposit slips and annual financial statements); and
• Shipping and receiving documents (e.g., manifests and bills of lading).

Developing a clear picture of where documents are located is also important, whether they are in file cabinets, shared network servers, e-mail servers, laptops or tablets, or other physical items such as flash drives and disks, they should all be included in the written document retention policy.

If your company has a bring-your-own-device (BYOD) policy, make sure that it is compatible with the document retention policy. If there is not a BYOD policy currently in place, include language regarding the use of personal devices for company business.

Identify who should be responsible for records and whether that responsibility is centralized in one department or person, spread amongst the company’s business departments, or shared by employees on a records/document retention/information governance task force.

Review State & Federal Rules on Document Retention Requirements
There is no universal law for document retention and usually, for certain types or categories of documents and/or companies, regulatory or statutory rules dictate retention periods. For example, the SEC requires that all SEC-regulated companies retain e-mails for at least three years,¹ and the IRS has various requirements on the length of time that tax records and supporting documentation must be kept.

States that have adopted the Uniform Preservation of Private Business Records Act² include Colorado, Georgia, Illinois, Maryland, New Hampshire, Oklahoma, and Texas. If your company's home state has adopted this uniform legislation, ensure that the definition of business record is included in your written document retention plan.

Documents necessary for pending litigation may need to be retained and preserved beyond regulatory or statutory rules. Those duties arise only when the company has a reasonable notice of pending litigation, and then a “litigation hold” – a suspension of the usual document destruction rules to preserve documents for potential litigation – must be put in place. Researching the legal requirements for retention across different categories of documents can be difficult, so be sure to note the research process and consult counsel as necessary.

Create a Retention Schedule & Instructions on Storing, Retaining & Preserving Data
Once the research into legal retention requirements is done, a retention schedule should be set for all document types that your company handles. This schedule should include details on how and when the documents are organized, stored, retained, backed up, and destroyed. Courts have advised that companies (even those with frequent litigation) are not required to keep every “shred of paper, every e-mail or electronic document, and every backup tape…Such a requirement would cripple large corporations.”³

Therefore, outside of regulatory, statutory, or industry regulations as well as any impending litigation and related “litigation hold,” your company is free to develop its own retention policies. In other words, you only need to keep e-mails and other categories of ESI for as long as you deem appropriate. Once the policy is established, it must be strictly adhered to for it to remain reasonable.
Set Rules on Destroying Expired or Useless Data

Many companies permanently delete e-mails and similar electronic data (chats, calendar appointments, etc.) on a consistent schedule.

From a litigation viewpoint, such a policy can be sustained if it is applied consistently and if it is suspended during a “litigation hold.” This policy must weigh the company’s business needs, IT considerations, and the balance between saving important e-mails and deleting extraneous ones.

The key, once again, is the consistent implementation of the policy once established. For example, some companies automatically delete e-mails older than three months unless it is specifically saved by an employee, saved pursuant to a management directive, or saved as a part of the automated document management system.

This practice has been accepted by courts, which have recognized that routine data destruction policies are appropriate even when they may result in the destruction of documents that might turn out to be relevant in a later lawsuit, as long as the lawsuit was not reasonably foreseen at the time of the destruction.

This aspect of the retention policy will undoubtedly have various technical considerations. For example, software is available that can search for keywords or phrases deemed sensitive by management, mark such e-mails for retention, and mark any e-mails that are manually saved by employees.

Automatically deleting e-mails on a time schedule is one way to ensure that the document retention plan is being consistently implemented. Deleting unneeded data on a time schedule can help lessen the risks of a potential data breach (less data to lose) and can help streamline future data requests.

Whether or not an automatic e-mail deletion scheme is used, the policy also needs to specify procedures on how to destroy expired documents or data beyond e-mail that is no longer needed. Taking the time to think through what archival data is useful to the company and how it can be used is an important step in developing a good document retention policy. This is also another reason to consider involving the stakeholders across the company in the development process.

Rather than keeping everything, weigh the potential benefits of retaining data for research, development, or historical purposes against the costs and risks of retaining that data. The policy should also specify how the destruction of documents will be suspended when exceptions such as a litigation or another hold is initiated.

Litigation Holds & Other Exceptions

The importance of a solid written document retention policy can shine through when circumstances require an exception to its rules and a hold must be put into place.

Litigation holds are perhaps the most common and most discussed exception to document retention policies because, when litigation is reasonably anticipated, a company has a duty to preserve information relevant to that litigation.

The basic steps to a litigation, or any other type of hold, are to:
1) Identify employees with relevant data;
2) Inform the employees of the duty to preserve;
3) Suspend any automatic deletion systems;
4) Provide instructions for preserving data;
5) Document and monitor the process; and
6) Release the hold when appropriate.

A rumor or possibility of litigation is not necessarily enough to trigger the duty to preserve. However, in addition to receiving a complaint, petition, or the filing of a suit, there are many other potential events that give reasonable notice to a company. Receiving a letter from a contractor that points to a possible suit, a notice of administrative complaint, a government inquiry, a third-party document request, an internal grievance, or a human resource (HR) dispute could all potentially trigger a duty to preserve and the necessity to implement a litigation hold. Your company is also reasonably aware of potential litigation if it is seriously contemplating or taking action to initiate litigation.

As soon as there is reasonable anticipation of litigation and the duty to preserve relevant information, the litigation hold process must be put into action. The hold process must begin by identifying the sources and locations of relevant information. Identifying the people who will have the relevant information, also known as “custodians” of the data, is critically important so they can find and preserve the relevant data and dispose of any irrelevant clutter.

A litigation hold memo must be issued in writing, and a variety of additional communication methods can be considered, but a minimum of e-mail distribution with read receipts is recommended. Issuing the litigation hold memo to the identified custodians is an absolute minimum, but company-wide distribution is recommended practice.

For the identified and relevant custodians, any existing automatic e-mail and/or file deletion systems must be deactivated.
for the duration of the litigation hold. The previous exercise of taking inventory of the document locations becomes especially helpful and makes the litigation hold process easier.

Determine the locations of the data that must be preserved using the data inventory from your document retention policy and additional interviews with the data custodians. After identifying and taking inventory, issue additional instructions to the custodians regarding their duty to preserve and comply with the litigation hold, continuing to document the process throughout each step.

After the initial issuance of the litigation hold, the best practice is to remind the custodians involved (and anyone else with access to relevant data) of the duty to preserve on a periodic basis. This can be done via reissuance of the original notice, pop-up messages, voice mails, or posted reminders. Monitor and audit the process throughout the duration of the litigation hold.

The litigation hold can be released once litigation is no longer reasonably anticipated or has concluded, whether by a court-entered dismissal with prejudice, a final judgment where the time for appeals has ended, or when a final settlement and release has been signed. Deciding when litigation is no longer reasonably anticipated and when the hold may be released is less clear-cut but may also involve a settlement of some kind. Courts have looked for whether the release decision is based on a good faith and reasonable evaluation of the facts and circumstances known at the time.

After the hold is released, normal document retention (and destruction) policies for all data and custodians involved should be restarted. Just as it was with the implementation of the litigation hold process, all steps of the hold release should be documented.

In addition to litigation holds, there are other exceptions or hold situations where the document retention policy must be suspended. These exceptions can include tax audits, government investigations, and business-related scenarios such as mergers or acquisitions, bankruptcies, or technology reviews. Your company may also enter into contracts that require holding specific documents or data for certain amounts of time (e.g., until a construction project is completed), and those contractual hold requirements should also be tracked.

**Implement Document Retention Training**

Training employees on the document retention plan is a crucial implementation step and should not be treated as an afterthought. A training program should be developed and available at the time of implementation with written materials available. Special events or exceptions, such as litigation holds or audits, should be discussed during the training.

Because systematic and consistent compliance with the plan is important, discuss penalties for noncompliance as well. Clear instructions on employee document retention and disposal procedures should be addressed both at the implementation of the policy and while training new employees.

**Review Policy & Update Periodically**

Once a document retention policy is implemented, it is good practice to periodically revisit and update it. This is especially true with the speed at which technology changes because, as new tools become available or are in common use, you may have to cover additional data sources in your policy. Changes in state and federal rules or case law may also influence your policy, so a regular check with legal counsel can assist you in managing risk.

**Conclusion**

A well-constructed and consistently applied document retention policy can save your company storage costs, help manage the risks of a data breach, and assist in easing the burden of discovery in the event of a litigation. While the process may be daunting, the benefits to creating such a policy are worth it.
Endnotes


KELLEY J. HALLIBURTON is an Attorney in the litigation, construction, and government contracts groups at Shapiro, Lifschitz & Schram located in Washington, D.C. She has extensive experience in all aspects of electronic discovery including managing significant volumes of electronically stored information (ESI), utilizing various electronic review platforms and litigation support systems, and managing the firm’s electronic discovery department.

Phone: 202-689-1900
E-Mail: halliburton@slslaw.com
Website: www.slslaw.com