

Should I Shred This?

David R. Brown, Associate
Gould & Ratner

Most business owners and managers are at least minimally familiar with the concept of document retention policies (“DRPs”). Unfortunately, this acquaintance may stem more from egregious examples of DRP abuse than from a genuine appreciation of their value. The recently ended trial of Frank Quattrone, a former star dot-com investment banker, focused on the aggressive enforcement of a DRP as a tool to obstruct an official investigation. Just a year previously, the collapse of Arthur Andersen demonstrated that document shredding in the face of a criminal investigation is a poor idea. These unfortunate episodes raised awareness of DRPs, but did little to demonstrate when information may be destroyed legally and why it should in fact be destroyed. In this context, it is important to review why and how an honestly-run business may benefit from a DRP.

What is a DRP?

DRPs are formal, written guidelines by which a company determines when and for how long it will retain particular types of information, after balancing a number of competing considerations. Important factors to consider include the usefulness to the company of older data, legally mandated retention periods, and the potential for disclosure of sensitive or harmful internal records should the company become a party to a lawsuit. Adopting and enforcing a DRP necessarily involves

Gould & Ratner
222 North LaSalle Street, Suite 800, Chicago, Illinois 60601

PROFESSIONAL RULES IN SOME JURISDICTIONS MAY TREAT **TAKING STOCK AS ADVERTISING**. ALSO, PLEASE NOTE THAT WHILE THE ABOVE IS INTENDED TO BE A PUBLIC SERVICE ANNOUNCEMENT, IT MAY BE CONSTRUED UNDER THE "CAN-SPAM" ACT OF 2003" TO BE A "COMMERCIAL ELECTRONIC MAIL MESSAGE" AND , IF IT IS SO INTERPRETED, THE ABOVE MESSAGE MAY BE CONSIDERED "ADVERTISING" UNDER SAID ACT.

If you have received this message in error and/or if you wish to be removed from our list, please reply with "remove" in the subject line of your email. We apologize for any inconvenience.

destroying company records, even those which might someday be useful. Many successful businesses have determined, however, that the benefits of adopting and enforcing a DRP far outweigh those of the alternative “pack-rat” approach.

Who Needs a DRP?

All businesses should consider adopting a DRP. An ideal business would retain complete, relevant, compact, indexed and searchable information, and restrict access to this information to the company itself. In such an environment, a DRP would be unnecessary. The real world, however, hardly resembles these laboratory conditions. A typical business may generate thousands of paper and electronic documents, emails, voicemails and instant messages per employee per year. Often these materials contain inaccurate, irrelevant, outdated and/or potentially incriminating information. At times, such information may exist only in documents residing on a particular media. For example, electronic documents may contain non-obvious “metadata,” such as previous drafts, internal comments and other matter not intended for dissemination. This background information does not appear when the final document is printed. Similarly, paper versions of documents may bear marginalia absent from their electronic counterparts. Unless disposed of according to a rational, consistently-applied DRP, data either 1) remains in the company’s files, open to inspection by opposing parties in litigation and government regulators armed with subpoenas, or 2) is destroyed or discarded in a haphazard fashion, losing later-needed important information or exposing the company to charges of destroying evidence. No business can claim perfect knowledge of what lurks in its aging files. Operating without a DRP consequently presents unquantifiable risks.

What Should a DRP Cover?

A well-conceived DRP will provide a high degree of certainty as to what information a company possesses at any point in time. Specifically, it must address five distinct areas of concern.

First, the DRP should not materially interfere with normal business operations. Second, it must address all forms of data – it does little good to mandate the destruction of paper documents if electronic versions reside indefinitely on servers and backup tapes. Third, it must comply with laws of general application which mandate document retention and have regard for any relevant statutes of limitation. Fourth, the DRP must take account of industry-specific regulations. Finally, a company must recognize that slavish compliance with its DRP rules in the face of an official investigation may be a crime, and therefore the DRP must contain procedures for stopping its application company-wide on short notice. A company which correctly synthesizes these factors into its DRP will benefit greatly from the regular destruction of the specified records and has little reason to fear allegations of misconduct.

How Long Should Documents be Retained?

As the considerations outlined above suggest, appropriate retention periods under a DRP will vary owing to the differences between industries as well as the corporate culture and risk tolerance of individual businesses. DRPs often mandate the following retention periods:

- Tax Returns and Records: Seven years, to allow for the expiration of the three year statute of limitations on negligent errors on returns and the six year statute on some forms of fraudulent returns
- Employment Records: Term of employment plus six to ten years, to allow for the expiration of the various statutes of limitations applicable to employment-related claims, including general contract and tort actions, as well as claims under employment-specific laws and regulations
- Policy Manuals: Ten years, to allow for the expiration of the statute of limitations for employment-related claims which refer to such policies

- Sales Records: Five to ten years, to allow for the expiration of the statute of limitations regarding enforcement of contracts
- Intellectual Property: Permanently, to protect against challenges which may be asserted at any time
- Real Estate Records: At least twenty years, to defend against squatters claiming adverse possession of real estate

Naturally, because statutes of limitations vary considerably by state, and because the risk and return trade-off between retention and disposal depend in large part upon local law, businesses should consult with their counsel before enacting a DRP to ensure that the protections sought are in fact obtained.

How Should a DRP Be Implemented?

The precise ingredients of a successful DRP will depend on facts and circumstances unique to the business in question. Generally speaking, the DRP should facilitate the legitimate operations of the business, save money by reducing the volume of records to be stored and searched, yet not obstruct justice or destroy evidence. Many companies have chosen to automate the electronic components of their DRPs by storing files in a central server or data center, categorizing them by type, and regularly and automatically purging files once the applicable retention period has expired. Similar methods can ease the compliance burden for paper files – central file storage and accurate records of file contents are key. Equally important is educating not only managers, but also rank-and-file employees concerning the implementation of the DRP.

What's the Bottom Line?

A DRP enacted in good faith and consistently applied saves time, money and aggravation by ensuring that a business retains only those files necessary for important business purposes and legal compliance. By separating wheat from chaff, it reduces the burden of file storage, shrinks the

universe of potentially harmful information available to outsiders, and imposes order on rapidly multiplying paper and electronic records.