



Point, Click, Retain?

In today's digital age, companies must have a well-defined electronic record retention policy

by **Pamela V. Rothenberg**

In two separate cases decided in July, federal district courts ordered sanctions against corporations after finding employees failed to retain e-mail messages in accordance with the companies' document retention policies.¹ These rulings underscore the risks companies face if they fail to develop, implement and enforce meaningful electronic record retention policies. Courts are no longer sympathetic to claims of ignorance about the destruction of relevant electronic documents. Those without comprehensive policies face exposure to dangerous and expensive discovery demands in litigation, obstruction of justice charges, fines and penalties and potentially ruinous claims of destruction of evidence in litigation.

Electronic files present unique challenges. An electronic record retention policy is a set of guidelines and procedures to determine how long a company should keep its records, including e-mail, electronic files and Web pages. It should be in writing and clearly spell out a procedure to systematically address records. Having no policy is a policy in and of itself—and a bad one at that.

A policy should specifically identify the records to be retained and deleted (and when destruction should occur). It should also include the reasons for having the policy so employees can make more educated decisions

regarding deletion or retention. The policy should classify different types of documents (tenants' financial information, employee records, payroll/accounting records, tax records, contracts, repair records, etc.) and detail how long to keep each type.

The policy should classify different types of documents and detail how long to keep each type.

The policy should also specify the manner for retention. Should the documents be held on the company's server or on an employee's hard drive? Policies must also take into consideration separate regulatory requirements, in particular those relating to accounting, medical, legal, pharmaceutical, securities and government/public records.

To be effective, a policy must be enforced—a poorly implemented policy can be more dangerous than having none at all. Companies must adjust the manner in which the policy is enforced depending on different timing issues: if no litigation is pending and no lawsuits threatened, the policy can be more liberally

created and enforced; where litigation is pending, the policy and its implementation must be strictly scrutinized; where no litigation is pending, but a lawsuit has been threatened, the company's duty to retain documents will likely change, and it should seek the advice of legal counsel before proceeding with enforcement. Companies should consider establishing a compliance committee or manager whom employees may approach with questions.

It is critical for companies to develop, implement and systematically enforce an electronic records retention program in the regular course of their business, rather than in response to litigation. This will ensure the policy has been established for innocent purposes, especially where the stated objective of the policy is cost and resource control. Companies that are not proactive will likely be caught off guard, and the consequences can be severe. □

Pamela V. Rothenberg (prothenberg@wcsr.com) is a member of the real estate development and real estate technology groups at Womble Carlyle Sandridge & Rice, PLLC.

Lisa Ruddy (lruddy@wcsr.com), a member of the real estate development group at Womble Carlyle, substantially contributed to this column.

¹ See *Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243(SAS) (S.D.N.Y. July 20, 2004), and *U.S. v. Philip Morris USA Inc.*, 327 F. Supp.2d 21 (D.D.C. 2004).