

## **Electronic Document Retention Policies: A Business Necessity**

The news is full of stories of suspicion and liability due to missing electronic files: Missing emails from Karl Rove; deleted emails from Arthur Anderson; \$29.2 million award in a discrimination case after jury was instructed to “infer that [missing emails] would have been unfavorable.”

As a result of recent changes to the federal court rules, lawyers recommend that all companies have a written electronic document retention policy. At some point, most businesses can expect to be asked to produce electronic documents. Failure to do so can result in sanctions or an instruction to the jury against the company. Under the new rules, all parties must disclose their electronic documents or information about those documents, including where they are kept, early in a case.

Importantly, the new rules contain a safe harbor if electronic information was “lost as a result of the routine, good-faith operation of an electronic information system.” A company is protected from adverse instructions, or even a presumption of wrong-doing, if documents were destroyed in accordance with a written policy. Because of this, all companies should have a policy regarding the retention and destruction of electronic information, including emails.

Many companies instinctively respond with a strict destruction policy that provides for the earliest destruction of documents possible. They do so because companies have been held liable for millions of dollars or settled cases of discrimination or harassment, patent infringement, or anti-trust, based largely on incriminating emails. Of course, those cases involved companies where there was wrong-doing, the emails merely preserved the evidence.

However, companies not guilty of wrong-doing need to be concerned about favorable evidence that could be lost or selectively disclosed. The company that deletes email or files too quickly may leave itself without the proof necessary to fend off a suit. An employee suing about harassment, for example, can be expected to copy incriminating emails, like sexual jokes from a co-worker, but not exculpatory emails, such as the employee’s response of “LOL” (“laughing out loud”) or suggestive emails he or she initiated. Without an accurate email record, an employee could claim to have been harassed by email or to have reported harassment by email and the company has no means to disprove the claim.

Additionally, the failure to keep documents, even based on a uniform company policy, can result in liability. The former Wet N Wild water park had a standard policy to destroy all incident reports at the end of each season. The Nevada Supreme Court found the park was subject to the presumption that the documents, if they existed, would be adverse because the park destroyed evidence before the statute of limitations had run.

To avoid this presumption, an electronic document retention policy must require keeping all relevant records until the possible statute of limitations has run. But that time

frame depends on the content of the documents. A meaningful policy must provide a means of sorting the documents, a filter that will screen for sensitive emails and files and keep the relevant ones. The policy must cover all electronic devices, including PDAs, laptop computers, and possibly home computers, if company business is conducted on them. The policy needs to be crafted with the assistance of counsel and IT experts. Then it must be faithfully implemented, including audits to ensure compliance. Failure to do so could leave a company in the worst of all positions, without the evidence it needs to defend itself and yet subject to an adverse inference for failing to retain required records.

A good company need not fear its electronic records. Rather, it needs to plan what records to keep, how and where to keep them and how the records can be accessed if litigation does happen.