

Record Retention Policies: Guidelines for Directors

By Robert A. McTamanev and Richard G. Pierson

To enjoy the liability shield of the Business Judgment Rule, directors must have reliable business records as an essential predicate for their decisions. Record retention policies present a host of issues for directors, well beyond the retention and destruction procedures which well-managed businesses would adopt if commercial considerations, such as corporate governance and risk management, were the only criteria.

These policies are better described as “record destruction policies,” since their principal goal is to set a date when records can safely be discarded without fear of adverse consequences. In the *Arthur Andersen* case, the Supreme Court specifically confirmed that “[i]t is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.”

Whether retention will be beneficial or detrimental depends, of course, on the circumstances and the document itself. Employees should be educated on the specific risks associated with document preparation, and learn the consequences of producing detrimental documents. In mergers, for example, directors and management should assume that anything and everything written about the deal is subject to Section 4(c) filing with the Hart-Scott-Rodino pre-merger notice, and these writings could be a roadmap to an antitrust issue that simply might not otherwise occur to the antitrust regulators.

Director Summary: Directors must have reliable business records as an essential predicate for their decisions; however, in light of corporate governance and risk management considerations, record retention policies present a host of additional issues for directors.

Electronic Issues

Advances in wireless technology and user friendliness have resulted in e-mail becoming a primary form of communication. Thoughtless e-mails written in haste often come back to haunt the sender.

Federal Rules of Civil Procedure, revised in December 2006, have extensive and demanding e-data discovery rules, with early “meet & confer” requirements; negotiation of “easily accessible” and other e-data with possible shifting of discovery costs; privilege issues and safe harbors for good faith loss or destruction of relevant electronic records. While hard copies of documents are easy to destroy, electronic copies sometimes rise like the Phoenix from the ashes, often at the most inopportune times. Presently there are procedures to render electronic files unrecoverable, but forensic recovery methods are constantly becoming more sophisticated. And if records exist and are destroyed or not produced after a proper demand is made, penalties can include judicial sanctions and even dismissal of the case.

To Keep or Destroy?

In general commercial litigation, immediate holds are put on document destruction, but with an automatic destruction program in place it might be too late to save an important document. Most substantial corporations are constantly involved in various litigations, so determining the proper depth of a direction to hold all documents might be difficult or impossible to assess until after the fact.

Even given the substantial costs of document archiving, there can be advantages to retention and explanation of a troublesome document, as opposed to destruction with possible adverse inferences or worse. Applying this general concept to real world practice is extremely difficult. The relatively modest cost of electronic retention, versus the time and manpower cost of implementing and maintaining a disciplined destruction program, results in many businesses keeping everything virtually forever—and in



the process subjecting all documents to future discovery requests, and often presenting only a possible litigation liability with little or no business value.

A thorough record retention policy provides guidelines and procedures for storage, organization, retrieval and, ultimately, destruction of documents. Documents may be retained (1) never, (2) forever, or (3) for designated time periods, depending upon the nature of the document and the rationale for its retention, if at all. The policy designates the individuals responsible for compliance with the policy and provides for the immediate suspension of the policy in the event of litigation, an investigation, or other designated events.

Compliance Considerations

First, there are U.S. legal requirements to maintain certain records for designated periods, and to provide them to government agencies under certain conditions. For example, Sarbanes-Oxley requires the auditors of U.S. public companies to retain their audit workpapers and related information for seven years after the relevant audit's conclusion. SOX also criminalizes the destruction or alteration of documents by anyone with the intent to obstruct a government proceeding. Second, there are basic corporate records and important agreements and other documents which should be retained and safeguarded. Finally, as noted above, there are evidentiary and discovery requirements in the event that the company becomes involved in litigation or regulatory proceedings.

The instant that litigation or regulatory proceedings become reasonably foreseeable, an immediate hold must be imposed on all possibly relevant documents and sources. In the case of a corporate client with diverse operations, it may be virtually impossible to conclude with confidence that a record in one location can be destroyed, since the possibility might exist that it is relevant to or subject to discovery in a case or proceeding in another jurisdiction far away. When the documents no longer exist, or when the disks have been wiped clean or are otherwise not recoverable, the typical inference is that the result was intended, and that the information destroyed would have been adverse to the destroyer. "Litigation Holds" are also relevant to a later claimed attorney work product privilege, since both should be triggered contemporaneously at the time litigation is reasonably anticipated.

Documents Can Live Forever

Remember that anyone who has had access to the document likely also has had the opportunity to print it or to send a copy to another computer or file, and it is obviously no defense to a discovery request to argue that a relevant document should have been destroyed and that

While hard copies of documents are easy to destroy, electronic copies sometimes rise like the Phoenix from the ashes, often at the most inopportune times.

a copy was retained in violation of corporate policy. Furthermore, index information describing the discarded document may be retained long after the document itself has been wiped clean or overwritten.

Conclusion

In summary, prudent corporate planning would suggest the following caveats:

1. Unless a law says otherwise, there is no law against a Document Destruction Policy.
2. If a document has been created, assume that a copy of it exists somewhere.
3. If a document has been created electronically, assume that it can be retrieved.
4. When in doubt, ask. When really in doubt, ask in writing, and save the answer.

Because of the importance of record retention policies, and the dire consequences which could result from the retention of a document better destroyed, or the destruction of a document which should have been or which was required to be retained, the policies should be reviewed and approved by senior management and the board in consultation with in-house general counsel and outside legal counsel. The policy should be acknowledged by all relevant employees and should be enforced consistently. Violations, in the form of either early destruction or late retention should be treated seriously and should be remedied and disciplined.

The following sidebar provides a Model Records Retention Policy for use by a publicly held corporation in the U.S. subject to Sarbanes-Oxley. It is a model, and must be adapted to the facts, requirements, and risk profile of a company considering its adoption. ■

Robert A. McTamaney is a partner and chair of the corporate department, and **Richard G. Pierson** is a partner and member of the corporate department, at Carter Ledyard & Milburn LLP.



Model Records Retention Policy

Note: This model must be adjusted to the specific business with advice of counsel.

Records Policy

The records of the Company are important assets. Corporate records include essentially all records you produce as an employee, whether paper or electronic, and e-mail specifically.

Failure to retain records for the minimum periods required by law could subject you and the Company to penalties and fines, cause the loss of rights, obstruct justice, spoil potential evidence in a lawsuit, place the Company in contempt of court, or seriously disadvantage the Company in litigation.

Sarbanes-Oxley requires the auditors of public companies to retain their audit workpapers and related information for 7 years after the audit's conclusion. SOX Section 1102 states that anyone who corruptly: (i) alters, destroys, mutilates, or conceals a document, or other object or attempts to do so, with the intent to impair its use in an official proceeding; or (ii) otherwise obstructs any official proceeding, or attempts to do so, shall be fined, or imprisoned not more than 20 years, or both.

The Company's [General Counsel's Office] has been delegated responsibility for this Policy and for education of employees, working with the Information Technology and Records Departments to ensure compliance; periodically updating this Policy; and the coordination of destruction holds in appropriate circumstances.

The Company's General Counsel's Office will also advise regarding the U.S. Federal Rules of Civil Procedure, effective December 1, 2006, which regulate the discovery of electronic-stored data by the Company and by every relevant employee.

This Policy applies to all Company records, or copies or excerpts or summaries of such records, whether retained on site, off-site, in a personal computer or other device, or otherwise in employees' business or personal files. This Policy applies specifically to e-mail and instant messages, and to Company-related documents created by employees personally and not during active employment hours.

There are three kinds of Company records—**Temporary**, **Final**, and **Permanent**.

Temporary Records

Temporary records include all business documents that are intended to be superseded by Final Records or Permanent Records.

Temporary records shall be destroyed or permanently deleted if in electronic form when a project or matter closes.

Upon closing of temporary files, make sure that you have duplicates of all the final records and then destroy the temporary records.

Final Records

Final records include all business documents that are not superseded by modification or addition, including but not limited to documents given (or sent via electronic form) to any third party not employed by the Company, or to any government agency; final memoranda and reports; correspondence; handwritten telephone memoranda not further transcribed; minutes; specifications; journal entries; cost estimates; etc.

All accounting records shall be deemed Final Records.

Except as otherwise provided in the Document Retention Schedule and as otherwise defined by legal and regulatory requirements, all final records are to be discarded ten years after the close of the project or matter.

Permanent Records

Permanent records include all business documents that define the Company's scope of work, expressions of professional opinions, research and reference materials. Such include, but are not limited to contracts, proposals, materials referencing expert opinions, financial statements, tax returns, payroll registers, copyright and trademark registrations, patents and other documents relating to intellectual property rights, environmental reports, real estate records, and formal minutes of meetings.

Except as provided in the Document Retention Schedule, all permanent documents are to be retained indefinitely.

Record Maintenance and Storage

All physical records are maintained by the Records Department. All electronic versions of records are maintained within the Company's centralized electronic record software database, which is maintained by the IT Department.

The originals of all physical records—including tangible items such as photographs and audio or video recordings—should be *immediately* forwarded to the Records Department, to be dated, indexed, and placed within the project file.

When a project is completed, the Records Department will confirm with all employees working on that project that all original Final Records and Permanent Records related to that project have been placed in the project file.

The Records Department shall maintain an up-to-date list of all records stored on-site and off-site, along with the dates of the records' creation and project's completion. Based on that list, the Records Department will dispose of



records upon the expiration of each record's retention period, as outlined in the Document Retention Schedule or otherwise in this Policy.

Electronic records shall be maintained electronically. In the event that an electronic record is printed, the printed version shall be classified as a Temporary Record, Final Record, or Permanent Record and disposed of accordingly.

Company employees are not to store any records on the local hard drives of their Company-assigned computers, or on any non-Company computers or portable drives. Records should only be saved in the Company's software.

Disposal of Records

Physical records disposed of pursuant to the retention periods specified in the Document Retention Schedule shall be disposed of using a cross-cut shredder. The Records Department shall adopt procedures to permanently dispose of any non-paper physical records, such as photographs or audio/video recordings, and electronic records.

Hold on Record Destruction and Deletion

If a lawsuit or other proceeding involving the Company is reasonably foreseeable, all destruction of any possibly relevant documents, including temporary documents and e-mail, must cease immediately, and relevant documents will then be retained and organized under the supervision of the General Counsel's Office.

Violation of this aspect of the Company's Records Retention Policy could subject the Company and the employees involved to civil and criminal penalties.

Once the "Litigation Hold" is in place with respect to the designated files and documents, regular disposition of non-affected records should resume. The General Counsel's Office will advise regarding termination of any Litigation Holds in place, and regarding the future disposition of affected records.

E-mail Policies

All electronic communication systems as well as all communications and stored information transmitted, received, or contained on the Company's information systems are the property of the Company. Employees may not use a password, access a file, or retrieve any stored communication, unless authorized to do so. Employees have no expectation of privacy in connection with the use of Company equipment or with the transmission, receipt, or storage of information using the Company's equipment. Authorized Company personnel may access communications and stored information at any time without notice or consent.

Legal Requirements

Age Discrimination in Employment Act (ADEA) requires indefinite retention of ADEA-relevant records.

Civil Rights and Equal Pay Act requires retention of records for 1 year from the action date or the record preparation date.

ERISA records must be retained for 6 years.

Fair Labor Standards Act requires retention of virtually all employee information for 2 or 3 years.

Gramm-Leach-Bliley Act of 1999 and related FTC "**Safe-guards Rules**" have broad retention and protection requirements for private data of individuals, and apply to "financial institutions" as broadly defined.

Health Care and Insurance Portability and Accountability Act of 1996 and the related **HIPAA "Privacy Rule"** require retention and protection of employee health information.

INS Legislation prohibits hiring unauthorized aliens and to verify identity and employment eligibility.

IRS requires employment tax and Social Security Records to be maintained for 4 years after due date.

Federal Trade Commission rules require retention related to consumer privacy and security programs which the FTC enforces.

OSHA requires records of employees exposed to toxic agents and harmful substances to be retained for 30 years.

Sarbanes-Oxley Act of 2002 established broad certification and controls requirements which require intense documentation and retention of records (sections 302 and 404) and criminalize document destruction intended to obstruct official proceedings.

Title VII of the Civil Rights Act of 1964 requires indefinite retention of records relating to possible unlawful employment practices.

Welfare and Pension Plans Disclosure Act requires retention of reports for 5 years.

Note: Specific regulated businesses are subject to further requirements, and foreign, state and local laws and regulations impose further requirements, such as the EU Privacy Directive. Relevant statutes of limitations in foreign countries will vary from those in effect in the U.S.

Ed. Note: Directors Monthly articles do not constitute legal advice. In adapting this model, the advice of a competent professional should be sought.