

Corporate Department

Attorney Advertising

January 2009

Record Retention Policies

Record Retention Policies present a host of issues, well beyond the retention and destruction¹ procedures which well-managed businesses would adopt if commercial concerns such as corporate governance and risk management were the only considerations. Furthermore, 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 financial or other adverse consequences.

Whether a particular document's retention will turn out to be beneficial or detrimental depends on the circumstances and the document itself. A separate education of employees is required to avoid the preparation of potentially detrimental documents. For example, despite constant reminders, thoughtless e-mails written in haste often come back to haunt the sender.

The Federal Rules of Civil Procedure, revised in December 2006, have extensive and demanding e-data discovery rules, with early "meet & confer" requirements and schedule agreements, negotiation of "easily accessible" and other e-data, with possible shifting of discovery costs, privilege issues, agreement on the forms of production of e-data and records, and safe harbors for good faith loss or destruction of relevant electronic records. The new rules will require counsel to become quickly expert regarding every aspect of their client's record retention policies and procedures.

Under new FRCP 26(f), parties must "meet and confer" within the earlier of 99 days after filing the complaint or 69 days after the first responsive pleading. This requires immediate assembly of the legal and business team and advisers, identification of the "most knowledgeable" persons, and an immediate plan for e-discovery and implementation of the "litigation hold." The retention policy must be analyzed with the IT staff, who will be critical in the process, and corrected if necessary to ensure adequacy and reliability.

Where in the world is the potentially discoverable data, and how is it stored and protected? Is the data reasonably accessible, and, if not, is it nonetheless discoverable if "good cause" is shown under FRCP 26(b)(2)? The accessibility burden is on the party resisting discovery. Is the "litigation hold" clear, correctly implemented, and enforced? Are the discovery review software and systems adequate, flexible

¹ There is nothing illegal in any broad sense about a document destruction program, even where possibly relevant documents are destroyed, as long as the later relevant litigation or proceedings were not reasonably foreseen at the time the documents were destroyed. See *Arthur Andersen*, 544 U.S. at 704 ("It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances."); *Samsung Elecs. Co. v. Rambus, Inc.*, 439 F. Supp. 2d 524, 543 (E.D. Va. 2006).

and protective of confidentiality? Inadvertent disclosures are now easier to “call back,” but are still best avoided to begin with.

FRCRCP Rule 37(f) now provides a “safe harbor” for documents inadvertently destroyed despite “good faith efforts” to maintain and abide by a record retention program. An effective program, in place and enforced, is required to claim this position, and can avoid adverse inferences and worse, as discussed below. Absent such a program, the safe harbor will not be available.

In summary, the new Federal Rules bring welcome improvements, but the core is an effective record retention program, in place and enforced, before the discovery requests arrive.

In mergers, our first caveat to the parties is to 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. In general commercial litigation, immediate holds are put on document destruction, but with an automatic destruction program in place, that might be too late to save an important writing, and most substantial corporations are constantly involved in various litigations, so that 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 are advantages to retention and explanation, as opposed to destruction with possible adverse inferences or worse. If a document is created which clearly presents an issue, then attach a contemporaneous explanation of it, and why it is incorrect or misleading. Then at least the record is there if the need ever arises. Applying this general concept to the real world is extremely difficult in practice.

On the other hand, the relative costs of electronic data retention, versus the often more expensive alternative of effecting a disciplined destruction program, result in many modern businesses keeping everything virtually forever, often in legacy systems which fall increasingly out of date, except as purely old record storage systems, but still are subject to future discovery requests, and often present only a possible litigation liability, with little or no current business value.

There are certain U.S. legal requirements to maintain certain records for designated periods, and to provide them to government agencies under certain conditions. 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.

A thorough Record Retention Policy provides retention guidelines and procedures for storage, organization, retrieval and, ultimately, destruction of documents; the policy designates the individuals

responsible for compliance with the policy; and finally the policy provides for the suspension of the policy in the event of litigation or an investigation or other designated events.

The typical Record Retention Policy divides documents broadly into two categories:

I. No Retention: Records which can be discarded immediately.

II. Designated Retention: Retention for specified periods, or permanently, as appropriate.

Since retention of hard copies and electronic documents is expensive and often time-consuming, the most common preference is toward discarding any documents that are not required to be maintained. Unfortunately, even a general destruction policy can sometimes raise adverse inferences in litigation, as discussed below.

Because of their importance, Record Retention Policies should be reviewed and approved by senior management, should be communicated to and 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 if appropriate. The client's General Counsel's Office should have a designated attorney or designated outside counsel to supervise the Policy, to interpret it in specific cases, and to supervise employees' training.

The Sarbanes-Oxley Act of 2002 and its regulations require the auditors of public U.S. companies to retain their audit work papers and related information for 7 years after the relevant audit's conclusion. SOX also contains two obstruction of justice provisions which criminalize the destruction or alteration of documents with the intent to obstruct a government proceeding. These SOX provisions apply to anyone and everyone, including public companies, private companies, their auditors and their lawyers and anyone else who violates the law. SOX Section 1102 states that whoever corruptly: (i) alters, destroys, mutilates, or conceals a record, document, or other object or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or (ii) otherwise obstructs, influences or impedes any official proceeding, or attempts to do so, shall be fined or imprisoned for not more than 20 years or both.

Deliberately withholding records obviously can attract sanctions and worse. In January 2008, a federal court ordered telecom giant Qualcomm Inc. to pay \$8.6 million in sanctions and asked the California state bar to investigate six of its attorneys for ethical violations after finding that it deliberately withheld nearly 50,000 documents from discovery in a patent dispute with rival Broadcom Corp. The court also ordered Qualcomm and its attorneys to undertake a comprehensive review of discovery failures in the case and develop a case-management protocol that would avoid similar scenarios in future cases.

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. There are presently 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.²

Logically, destruction of electronic records should raise no more of an adverse inference than destruction of hard copy records, provided that there then exists no reasonably foreseeable reason for further retention. However, 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.³

If records are discarded after a litigation or proceeding is reasonably foreseeable, it is simply no excuse to say that the documents were destroyed since the policy applied automatically,⁴ and the risk of sanctions or worse is present with electronic documents to exactly the same extent as with hard copies. All of the recent sanctions cases have involved failure to produce e-mails to some extent. And where the documents no longer exist, or where the discs 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.⁵ “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, and the hold directive itself typically is protected as either privileged or work product or both.

Remember as well 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 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.

² E.g., *Plasse v. Tyco Elecs. Corp.*, 448 F. Supp. 2d 302, 308-11 (D. Mass. 2006); *United States v. Tamez*, Nos. 06 Civ. 3111(DC), 03 Cr 1439(DC), 2006 WL 2854336, at *6 (S.D.N.Y. Oct. 5, 2006).

³ See, e.g., *Krumwiede v. Brighton Assocs., L.L.C.*, No. 05 C 3003, 2006 WL 1308629, at *8 (N.D. Ill. May 8, 2006) (“Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a litigation hold to ensure the preservation of relevant documents.”)

⁴ *Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988) (“a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy”).

⁵ See e.g., *Plasse v. Tyco Elecs. Corp.*, 448 F. Supp. 2d 302, 309 (D. Mass. 2006) (“Plaintiff argues that the inaccessible documents are not relevant and their deletion would therefore be meaningless. As the documents have disappeared, the court is in no position to assess this claim; the systematic destruction of these documents certainly suggests otherwise”). The leading adverse inference case is *Zubulake v. UBS Warburg LLC*, 229 FRD 422 (S.D.N.Y.. 2004), and the most prominent default judgment case is *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.* (Fla. Cir. Ct. 2005), where the compensatory and punitive damages exceeded \$1.4 Billion.

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.

Annexed to this summary is 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 and requirements and risk profile of a client considering its adoption.

If this discussion of Record Retention Policies prompts any questions, please contact **Robert A. McTamane**y (mctamane@clm.com) of our New York Office.

Carter Ledyard & Milburn LLP uses Client Advisories to inform clients and other interested parties of noteworthy issues, decisions and legislation which may affect them or their businesses. A Client Advisory does not constitute legal advice or an opinion. This document was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

© 2009 Carter Ledyard & Milburn LLP.

CL&M Model Record Retention Policy

[Name of Corporation]

Record Retention Policy

[This is a Model Policy, and should not be considered legal advice. The particular administrative and legal needs of your Company may not be addressed by this Model. Any organization considering implementing a records retention policy should first contact counsel to develop a plan suited for its specific business and unique situations that may arise, and then should adapt this Model to suit the Company's specific requirements.]

The corporate and business records of the Company and its subsidiaries are important assets. Corporate records include essentially all records you produce as an employee, whether paper or electronic. A record may be as obvious as a memorandum, an email, or a contract, or something not as obvious, such as a computerized desk calendar, an appointment book, or an instant message.

The law requires the Company to maintain certain types of records, usually for a specified period of time. Failure to retain those records for those minimum periods 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.

The Sarbanes-Oxley Act of 2002 and its regulations require the auditors of public U.S. companies to retain their audit workpapers and related information for 7 years after the relevant audit's conclusion. SOX also contains two obstruction of justice provisions which criminalize the destruction or alteration of documents with the intent to obstruct a government proceeding. These SOX provisions apply to anyone and everyone, including public companies, private companies, their auditors and their lawyers and anyone else who violates the law. SOX Section 1102 states that whoever corruptly: (i) alters, destroys, mutilates, or conceals a record, document, or other object or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or (ii) otherwise obstructs, influences or impedes any official proceeding, or attempts to do so, shall be fined or imprisoned not more than 20 years or both.

To ensure compliance with this Policy, the Company's [General Counsel's Office] has been delegated overall supervision and responsibility for this Policy and will coordinate education and training of employees, working with the Information Technology Department to ensure compliance with this Policy regarding electronic records; working with the Records Department to ensure compliance with this Policy regarding physical records; 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.

The Company expects all employees to fully comply with any published records retention or destruction policies and schedules. 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 and without limitation to e-mail and to instant messages, and to Company-related documents created by employees personally and not during active employment hours.

Broadly, there are two kinds of Company records- **Temporary** and **Retained**.

Temporary Records

Temporary records include all business documents that are intended to be superseded by final or permanent records, or which are intended to be used only for a limited period of time, including, but not limited to written memoranda and dictation to be typed in the future, reminders, to-do lists, reports, drafts, and interoffice correspondence regarding a client or business transaction.

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

Upon closing of such temporary files, gather and review all such temporary records. Before you destroy or delete these documents make sure that you have duplicates of all the final records pertaining to the project or matter. Upon destruction or deletion, organize the final records (and duplicates) in a file marked "Final" and store them appropriately, as required by this Policy.

Retained Records

Retained records include all business documents that are not superseded by modification or addition, including but are 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 are Retained Records.

Except as otherwise provided in the attached Document Retention Schedule, all Retained Records are to be discarded ten years after the close of the project or matter.

Some Retained Records will be retained permanently. These would 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.

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. Copies will be made available to employees as necessary.

When a project is completed, the Records Department will confirm with all employees working on that project that all original Retained Records related to that project have been placed in the project file. The Records Department will also confirm with all employees working on that project that any unnecessary duplicate copies of records in the project file, along with any Temporary Records related to the project, have been gathered and disposed of. The project file will then be transferred to the Company's off-site storage location.

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 will be treated as a physical record, and shall be classified as a Temporary Record or Retained Record and disposed of accordingly.

Electronic records must be placed into the Company's records retention software, which is available to all employees. When placing the record into electronic storage, the record type, creation date, and the related project or projects are entered into the system. Based on this information, and the retention periods identified in the Company's Document Retention Schedule or otherwise in this Policy, the software will automatically and permanently dispose of records at the expiration of their retention period.

The software will also generate a monthly report of records which do not fall into one of the record types listed in the Document Retention Schedule. The IT department, and if necessary any affected department heads and the General Counsel's Office, will classify these records and assign a retention period.

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. In the event that an employee needs to temporarily store

records outside the Company's software, the records should only be stored on Company-assigned computers with synchronization software.

The Company's software will automatically synchronize and back up calendars, task lists, and journal entries on a continuous basis.

Employees are not to use applications other than the Company's software to create or maintain Company records.

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.

In the event that it is necessary to manually dispose of an electronic record, the IT Department shall use the "permanent delete" function to permanently dispose of electronic records. In the event that records must be disposed of which are stored outside of the Company's software (in violation of this Policy), the IT Department must be contacted to permanently dispose of such electronic records.

Each employee's software has been configured to automatically delete any electronic trash cans/recycling bins when the computer is shut down. Similarly, the "deleted items" folder in each employee's Microsoft Outlook application has been configured to permanently delete all items in the folder each time the program is shut down. Employees are not to use these folders to store records, only to allow employees to immediately recover records which have been accidentally deleted.

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 e-mail, must cease immediately. Documents relating to the lawsuit or potential legal issue 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.

In the event of a Document Hold Direction, the IT Department shall immediately disable the "permanent delete" and "automatic delete" functions of the Company's software with respect to the designated records and disable the automatic deletion of recycle bins and deleted items folders on appropriate Company computers; the Records Department shall immediately suspend all disposition of records maintained on-site or off-site location as appropriate; and the General Counsel's Office shall immediately notify all appropriate employees by e-mail that they are not to dispose of relevant Temporary Records or other records until notified otherwise.

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 using this equipment for personal purposes do so at their own risk. Furthermore, employees may not use a password or passcode, 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.

E-mails not archived will be automatically deleted within 60 days. Employees should avoid using Company e-mail for personal purposes. Personal e-mails should be deleted as soon as possible.

E-mails relating to audit work papers and financial controls should be retained for at least 7 years.

All emails to the Company’s Officers or Audit Committee relating to complaints on auditing, accounting, frauds or internal controls should be retained permanently.

Any messages exchanged between the Company and third parties (such as consultants and auditors) should be archived, regardless of their content. Instant messages have the same status as e-mails and should be treated identically. IM should not be used for personal purposes.

Document Retention Schedule

Note: The Sarbanes-Oxley Act of 2002 and its regulations require the auditors of public U.S. companies to retain their audit workpapers and related information for 7 years after the relevant audit's conclusion. SOX also contains two obstruction of justice provisions which criminalize the destruction or alteration of documents with the intent to obstruct a government proceeding. These SOX provisions apply to anyone and everyone, including public companies, private companies, their auditors and their lawyers and anyone else who violates the law. SOX Section 1102 states that whoever corruptly: (i) alters, destroys, mutilates, or conceals a record, document, or other object or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or (ii) otherwise obstructs, influences or impedes any official proceeding, or attempts to do so, shall be fined or imprisoned not more than 20 years or both.

Document Type

Retention Period

ACCOUNTING/FINANCE

Audit Reports	Permanent
Audit Workpapers and related Accounts Receivable or Payable	7Y
Trial Balances	7Y
Analysis/Studies	7Y
Annual Operating Plans	7Y
Bank Statements/Reconciliations	10Y
Canceled Checks	10Y
Capital Expenditure Records	7Y
Capital Stock Book	Permanent
Cash Disbursement Journal	Permanent
Cash Receipts Journal	Permanent
Deposit Slips	7Y
Expense Reports	7Y
Expense Ledger	Permanent
Financial Statements	Permanent
Fixed Asset Detail	Permanent
General Ledger	Permanent
Inventory Records	7Y
Journal Vouchers	Permanent
Payroll Journal	Permanent
Payroll - Time Cards	7Y
Payroll - Earnings Records	10Y
Petty Cash Vouchers and related records	7Y
Prepaid and Accrued Expense Journal	7Y
Subsidiary Ledgers	Permanent

Voucher for payments to vendors, employees, etc. 7Y

CORPORATE RECORDS

Annual Reports	Permanent
Bylaws, Charter, Minute Books	Permanent
Capital Stocks and Bond Records	Permanent
Checks - Taxes, Property and Settlements	Permanent
Contracts/Agreements (still in effect)	Permanent
Contracts/Agreements (completed)	10Y
Trademark Registrations	Permanent
Deeds/Easements/Real Estate Records	Permanent
Labor Contracts	Permanent
Mortgages, Notes & Leases	10Y
Patents	Permanent
Retirement/Pension Records	Permanent
Tax Documents (all kinds)	10Y

CORRESPONDENCE

General	3Y (archive 4Y)
Legal & Tax	Permanent
License, Traffic, Purchase	7Y
Production	7Y
Routine - Vendor, Supplier, Customer	3Y (archive 4Y)

ENVIRONMENTAL

General Correspondence	10Y
Hazardous Waste Records	Permanent
Reports to ANY governmental agency	Permanent

INSURANCE

Accident Reports	7Y
Claims - After Settlement	7Y
Fire Inspection Reports	7Y
Disability Reports	7Y
Policies - Expired	Permanent
Safety Reports	7Y

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 “Safeguards 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 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. See I-9 retention.

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

Federal Trade Commission rules require consumers 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 specific requirements, and Foreign, State and Local laws and Regulations impose further specific requirements, such as the EU Privacy Directive. Relevant Statutes of Limitations in foreign countries will vary from those in effect in the U.S.].

MARKETING

Advertising	6Y
Business Development Documents	5Y
Consumer Relations	3Y
Distributors	3Y
Market Research	2Y
Presentations	
Internal	1Y
External	6Y
Product Development	10Y
Public Relations	8Y

OPERATIONS

Facility Plans/Blueprints	Permanent
Materials Management	5Y
Permits	Permanent
Quality Control	Permanent
Surveys	Permanent
Zoning	Permanent

PURCHASING & SALES

Pricing Information	Permanent
Purchase Orders	6Y
Sales Contracts	6Y
Sales - Domestic	5Y
Sales - Foreign	2Y
Sales Invoices	6Y
Sales Promotions	5Y
Sales Summaries/Reports	5Y

RESEARCH AND DEVELOPMENT

Products	Permanent
Projects	Permanent
Technical Papers	Permanent
Technical References	Permanent

SAFETY/OSHA

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

Disability Injury Reports	6Y
General Correspondence	3Y
Log of Occupational Illness and Injury	Permanent
Material Safety Data Sheets	Permanent
Occupational Incident Reports	Permanent
OSHA Record Keeping	Permanent
OSHA Safety Data Sheets	Permanent
Plant Safety Committee	Permanent
OSHA Health Standard Reports	Permanent
OSHA Noise Standard Reports	Permanent
Safety Bulletins	Permanent
Summary of Occupational Injuries for Calendar Year	6Y

TRAFFIC - Shipping and Receiving

Export Documents	10Y
Freight Bills	6Y
Manifests	6Y
Shipping and Receiving Reports	6Y
Bills of Lading/Waybills	6Y

PERSONNEL / HUMAN RESOURCES

Potential/New Employee Information

Employment Applications (Not Hired)	3Y
Employment Applications & Resumes (Hired)	Permanent
Employment Verifications	Permanent
Unemployment Compensation Data	Permanent
W-4 Tax Withholding Statements	7Y
Individual Time Sheets	3Y

Other Specific Legal Information

I9 and other Supporting Documentation	3Y
I9 and other Supporting Documentation (Terminated Employees)	1Y After Termination
Garnishments	7Y
EEO Charges/Cases	Permanent

EEO - Other Documents	3Y
EEO/Affirmative Action Plans	3Y
Exposure Monitoring Records	Permanent

Benefits Records

Medical Records (Enrollment and Change Forms)	Permanent
Worker's Compensation Claims	Current & Prior 4Y

Performance Related Records

Performance Appraisals	Current & Prior 4Y
Commendations Letters or Memos	Current & Prior 4Y
Disciplinary Letters or Memos	Current & Prior 4Y
Individual Attendance Records	Current & Prior 4Y

Prior Employees

Personnel Files (Terminated)	10Y After Term
------------------------------	----------------

Authorizations, Agreements and Miscellaneous Information

Contracts – Expired	7Y
Employee Communications	3Y
Professional Conduct Agreements	Permanent
Employment Offer Letter	Permanent
Orientation Checklist	1Y
Record or Exit Interview Discussion	Permanent
Handbook Acknowledgement	Permanent
Letter of Resignation	Permanent