Document Retention Policy

USA (National/Federal)

Related Content

A document retention policy (also known as a records and information management policy, recordkeeping policy, or a records maintenance policy) establishes and describes how a company expects its employees to manage company data from creation through destruction. It can be incorporated into an employee handbook or used as a standalone policy document. This Standard Document applies only to private workplaces. It is based on federal law. State or local law may impose additional or different recordkeeping requirements, but this document is relevant and useful to companies in every state. This Standard Document has integrated notes with important explanations and drafting tips.

GENERAL

Purposes of a Document Retention Policy

A **document retention policy** establishes and describes how a company expects its employees to manage company information (whether in electronic files, emails, hard copies, or other formats) from creation through destruction, according to applicable laws and the company's particular legal and business needs. It is one part of a company's overall document management program. To ensure that a document retention policy achieves a company's goals, counsel should tailor it to the company's specific needs and risk profile. No single policy is adequate for all companies. Companies with subsidiaries should compare their various retention schedules to inconsistencies with the parent company. It may make sense for some companies to have different retention schedules among subsidiaries if the subsidiaries are in different industries. Companies involved in mergers should conduct post-acquisition checks of record retention policies to determine where they may need to be made uniform with the parent company's policy.

A document retention policy serves many important functions. For example, it:

- Establishes that the company is committed to complying with all document retention laws. Several federal and state laws require companies to retain certain records and other types of information for a prescribed amount of time (for example, Rule 17a-4, Securities and Exchange Act; 29 C.F.R. § 1904.33; and Section 1085-2, Title 22, California Code of Regulations).
- Helps protect records that may be relevant to a pending or future law suit or government investigation from being destroyed before the discovery process.
- Describes how to comply with a **litigation hold**.
- Communicates employer expectations about which records employees may discard and when.
- Identifies who is in charge of record destruction, and explains how to notify the legal department and records management officer when a record is to be permanently destroyed.
- Encourages disposal of unnecessary files before they become a liability or unnecessarily costly to retain.
- Provides employers with a legal defense to some document production requests when certain records were previously deleted or destroyed.
- Sets up a way for a company to handle the potential consequences of a document retention failure.
- Provides direction on how personnel should manage information created or used as part of the company's business operations.
- Safeguards proprietary information, which can help companies manage and reduce operational and reputational risks.

Potential Legal Defense

A document retention policy reduces a company's likelihood of developing an unmanageable amount of information by providing a procedure for employees to discard legally most types of records. A document retention policy also may provide employers a legal defense in litigation if:

- Certain records relevant to a litigation or government investigation were previously destroyed by company employees or not backed up on company servers.
- The company exercised reasonable care to prevent and promptly correct any improperly destroyed information.

Drafting Considerations

A properly drafted and enforced document retention policy should:

- Require that employees suspend all disposal procedures during a litigation hold.
- Identify who employees should contact if they are unsure whether to dispose of a certain record.
- Include a records retention schedule.
- State that the employer will regularly audit employee files and email inboxes to ensure that employees are retaining and discarding records consistently with the company's policy.

Employee Training and Acknowledgment

All employees should be properly trained on document retention and litigation hold procedures to minimize instances of lost or improperly destroyed records. Training should begin during employee orientation and be repeated at least once annually. Each training session should be reinforced by having employees sign a certification acknowledging that they:

- Attended the training.
- Understand the document retention policy's requirements.

An acknowledgment section should be included in a stand-alone document retention policy to confirm an employee's receipt and understanding of its contents. If the document retention policy is part of an employee handbook, a single acknowledgment can be used for the entire employee handbook.

For more information on key issues relevant to drafting and enforcing a document retention policy, see Practice Note, Drafting a Document Retention Policy and Document Retention Policy: US Checklist. For a sample presentation to train employees on document retention and litigation hold procedures, see Document Retention: Presentation **Materials**.

Bracketed Language

The drafting party should replace bracketed language below in ALL CAPS with company-specific information. Bracketed language in sentence case is optional language that the drafting party may include, modify, or delete in its discretion. A forward slash between words or phrases indicates that the drafting party should include one of the words or phrases in the document.

DOCUMENT RETENTION POLICY

Reasons for Policy

The corporate information of [COMPANY NAME] [and its subsidiaries] is important to how it conducts business and manages employees.

Federal [and state] law require[s] [COMPANY NAME] to retain certain records, usually for a specific amount of time. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for [COMPANY NAME] and/or its employees:

- Fines and penalties.
- Loss of rights.

- Obstruction of justice charges.
- Inference of spoliation of evidence and spoliation tort claims.
- Contempt of court charges.
- Serious disadvantages in litigation.

[COMPANY NAME] must retain certain records because they contain information that:

- Serves as [COMPANY NAME]'s corporate memory.
- Has enduring business value (for example, it provides a record of a business transaction, evidences [COMPANY NAME]'s rights or obligations, protects [COMPANY NAME]'s legal interests or ensures operational continuity).
- Must be kept to satisfy legal, accounting, or other regulatory requirements.

[COMPANY NAME] prohibits the inappropriate destruction of any records, files, documents, samples, and other forms of information. This policy is in accordance with the Sarbanes-Oxley Act of 2002, under which it is a crime to change, conceal, falsify, or destroy any record with the intent to impede or obstruct any official or government proceeding. Therefore, this policy is part of a company-wide system for the review, retention, and destruction of records [COMPANY NAME] creates or receives in connection with the business it conducts.

REASONS FOR POLICY

Counsel may consider revising the clause above to include mention of any state or local law for the jurisdiction(s) where this policy will be used. Also consider adding examples of records that are specific to the company's industry and workplace.

Types of Documents

This policy explains the differences among records, disposable information, and confidential information belonging to others.

Records A record is any type of information created, received, or transmitted in the transaction of [COMPANY NAME]'s business, regardless of physical format. Examples of where the various types of information are located include:

- Appointment books and calendars.
- Audio and video recordings.
- Computer programs.
- Contracts.
- Electronic files.
- Emails.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Magnetic tape.
- Memory in cell phones and PDAs.
- Online postings, such as on Facebook, Twitter, Instagram, Snapchat, Slack, Reddit, Vine, and other social media platforms and websites.
- Performance reviews.
- Test samples.
- Voicemails.

Therefore, any paper records and electronic files, including any records of donations made online, that are part of any of the categories listed in the Records Retention Schedule contained in the Appendix to this policy, must be retained for the amount of time indicated in the Records Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Records Management Officer or the Legal Department.

Disposable Information Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed **materials** obtained from sources outside of [COMPANY NAME] and retained primarily for reference purposes.
- Spam and junk mail.

Confidential Information Belonging to Others Any confidential information that an employee may have obtained from a source outside of [COMPANY NAME], such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by [COMPANY NAME]. Unsolicited confidential information submitted to [COMPANY NAME] should be refused, returned to the sender where possible, and deleted, if received via the internet.

Mandatory Compliance

Responsibility of All Employees [COMPANY NAME] strives to comply with the laws, rules, and regulations that govern it and with recognized compliance practices. All company employees must comply with this policy, the Records Retention Schedule and any litigation hold communications. Failure to do so may subject [COMPANY NAME], its employees, and contract staff to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination.

Reporting Policy Violations [COMPANY NAME] is committed to enforcing this policy as it applies to all forms of records. The effectiveness of [COMPANY NAME]'s efforts, however, depends largely on employees. If you feel that you or someone else may have violated this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the [Records Management Officer/manager at the next level above your direct supervisor]. If employees do not report inappropriate conduct, [COMPANY NAME] may not become aware of a possible violation of this policy and may not be able to take appropriate corrective action. No one will be subject to and [COMPANY NAME] prohibits, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or cooperating in related investigations.

MANDATORY COMPLIANCE

It is important to remind all employees that retaliation of any kind, including for reporting any type of violation of a policy, is strictly prohibited. For more information on retaliation generally and how to prevent it, see Practice Note, Retaliation.

Records Management Department and Records Management Officer

The Records Management Department is responsible for identifying the documents that [COMPANY NAME] must or should retain, and determining, in collaboration with the Legal Department, the proper period of retention. It also arranges for the proper storage and retrieval of records, coordinating with outside vendors where appropriate. Additionally, the Records Management Department handles the destruction of records whose retention period has expired.

[COMPANY NAME] has designated [EMPLOYEE NAME] as the Records Management Officer. The Records Management Officer is head of the Records Management Department and is responsible for:

- Administering the document management program and helping department heads implement it and related best practices.
- Planning, developing, and prescribing document disposal policies, systems, standards, and procedures.

- Writing straightforward document management procedures to instruct employees on how to comply with this policy.
- Monitoring departmental compliance so that employees know how to follow the document management procedures and the Legal Department has confidence that [COMPANY NAME]'s records are controlled.
- Ensuring that senior management is aware of their departments' document management responsibilities.
- Developing and implementing measures to ensure that the Legal Department knows what information [COMPANY NAME] has and where it is stored, that only authorized users have access to the information, and that [COMPANY NAME] keeps only the information it needs, thereby efficiently using space.
- Establishing standards for filing and storage equipment and recordkeeping supplies.
- In cooperation with department heads, identifying essential records and establishing a disaster plan for each office and department to ensure maximum availability of [COMPANY NAME]'s records in order to reestablish operations quickly and with minimal interruption and expense.
- Developing procedures to ensure the permanent preservation of [COMPANY NAME]'s historically valuable records.
- Providing document management advice and assistance to all departments by preparing manuals of procedure and policy and by on-site consultation.
- Determining the practicability of and, if appropriate, establishing a uniform filing system and a forms design and control system.
- Periodically reviewing the records retention schedules and administrative rules issued by the governments of [NAMES OF RELEVANT STATES AND COUNTRIES] to determine if [COMPANY NAME]'s document management program and its Records Retention Schedule is in compliance with state [and foreign] regulations.
- Distributing to the various department heads information concerning state laws and administrative rules relating to corporate records.
- Explaining to employees their duties relating to the document management program.
- Ensuring that the maintenance, preservation, microfilming, computer disk storage, destruction, or other disposition of [COMPANY NAME]'s records is carried out in accordance with this policy, the procedures of the document management program and the requirements of federal and state law.
- Planning the timetable for the annual records destruction exercise and the annual records audit, including setting deadlines for responses from departmental staff.
- Maintaining records on the volume of records destroyed under the Records Retention Schedule and the records stored electronically.
- Evaluating the overall effectiveness of the document management program.
- Reporting annually to the Legal Department [and] [OTHER DEPARTMENT NAME] on the implementation of the document management program in each of [COMPANY NAME]'s departments.
- Bringing to the attention of the Legal Department any noncompliance by department heads or other employees with this policy and [COMPANY NAME]'s document management program.

RECORDS MANAGEMENT DEPARTMENT AND RECORDS MANAGEMENT OFFICER

For more information on the roles within the company that are responsible for implementing and managing the policy, see Practice Note, Drafting a Document Retention Policy: Define Employees' DRP Roles and Responsibilities.

How to Store and Destroy Records

Storage [COMPANY NAME]'s records must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to [COMPANY NAME]'s business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

STORAGE

This clause reminds employees to back up files necessary for the company's business continuation procedures. Counsel should consider revising the clause to include any records protected by state or local law for the jurisdiction(s) where this policy will be used. Also consider indicating the off-site location where duplicate files must be sent if physical copies are to be stored in a separate location, such as a storage facility.

Destruction [COMPANY NAME]'s [Records Management Officer/OTHER OFFICER/MANAGER] is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related records must be conducted by shredding if possible. Non-confidential records may be destroyed by recycling. The destruction of electronic records must be coordinated with the IT Department [TITLE].

The destruction of records must stop immediately upon notification from [the Legal Department] that a litigation hold is to begin because [COMPANY NAME] may be involved in a lawsuit or an official investigation (see next paragraph). Destruction may begin again once the Legal Department lifts the relevant litigation hold.

DESTRUCTION

A company's document management program and training procedures may include detailed instructions on how the Records Management Officer and other employees should destroy records. Once an employee destroys a record, he should document its destruction with the Records Management Officer, the Legal Department and other relevant personnel. The destruction of electronic records should be coordinated with the IT department to ensure that all copies of the electronic records are discarded, including copies residing on backup tapes, temporary files, additional servers, and all employees' email in-boxes and other electronic storage locations.

Litigation Holds and Other Special Situations

[COMPANY NAME] requires all employees to comply fully with its published records retention schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or [the Legal Department] informs you, that [COMPANY NAME] records are relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails, until [the Legal Department] determines those records are no longer needed. This exception is referred to as a litigation hold or legal hold, replaces any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may possibly apply, please contact [the Legal Department].

In addition, you may be asked to suspend any routine document disposal procedures in connection with certain other types of events, such as the merger of [COMPANY NAME] with another organization or the replacement of [COMPANY NAME]'s information technology systems.

LITIGATION HOLD AND OTHER SPECIAL SITUATIONS

This clause firmly states that the company's routine destruction procedures are suspended when its legal department implements a litigation hold (see Litigation Hold Toolkit). Counsel should remind employees periodically that they must immediately stop their regular deletion and disposal procedures when they are informed that the company is or may be facing litigation or government investigation (see Standard Document, Litigation Hold Reminder). When a litigation hold is to go into effect, counsel also should instruct the IT department to:

- Suspend any relevant auto-delete functions that affect the company's systems.
- Secure all information on company systems immediately.

Counsel may inform employees of these events by distributing a litigation hold notice (see Standard Document, Litigation Hold Notice). For more information on key issues that corporate counsel should consider when initiating a litigation hold, see Practice Note, Implementing a Litigation Hold.

Audits and Employee Questions

Internal Review and Policy Audits The chief financial officer and chief legal officer of [COMPANY NAME] [and the Records Management Officer] will periodically review this policy and its procedures with legal counsel [and/or] [COMPANY NAME]'s certified public accountant to ensure [COMPANY NAME] is in full compliance with relevant new or amended regulations. Additionally, [COMPANY NAME] will regularly audit employee files and computer hard drives to ensure compliance with this policy.

Questions About the Policy Any questions about this policy should be referred to [NAME] [(PHONE NUMBER; EMAIL ADDRESS)], who is in charge of administering, enforcing, and updating this policy.

[Acknowledgment of Receipt and Review

[I, _____ (employee name), acknowledge that on _____ (date), I received a copy of [EMPLOYER NAME]'s [NAME OF POLICY] and that I read it, understood it, and agree to comply with it. I understand that [EMPLOYER NAME] has the maximum discretion permitted by law to interpret, administer, change, modify, or delete this policy at any time [with or without notice]. No statement or representation by a supervisor or manager or any other employee, whether oral or written, can supplement or modify this policy. Changes can only be made if approved in writing by the [POSITION] of [EMPLOYER NAME]. I also understand that any delay or failure by [EMPLOYER NAME] to enforce any work policy or rule will not constitute a waiver of [EMPLOYER NAME]'s right to do so in the future. I understand that neither this policy nor any other communication by a management representative or any other employee, whether oral or written, is intended in any way to create a contract of employment. I understand that, unless I have a written employment agreement signed by an authorized [EMPLOYER NAME] representative, **I am employed at will and this policy does not modify my at-will employment status.** If I have a written employment agreement signed by an authorized [EMPLOYER NAME] representative and this policy conflicts with the terms of my employment agreement, I understand that the terms of my employment agreement will control.

OR

I, _____ (employee name), acknowledge that on _____ (date), I received and read a copy of the [EMPLOYER NAME]'s [NAME OF POLICY][, dated [EDITION DATE]] and understand that it is my responsibility to be familiar with and abide by its terms. [I understand that the information in this Policy is intended to help [EMPLOYER NAME]'s employees to work together effectively on assigned job responsibilities.] This Policy is not promissory and does not set terms or conditions of employment or create an employment contract.]

ACKNOWLEDGMENT

A signed acknowledgment of receipt, review, and understanding of any employee policy minimizes the potential for employees to later claim ignorance of that policy as an excuse for non-compliance. Although an acknowledgment included at the end of an employee handbook allows an employer to use one acknowledgment for all policies contained in the handbook, an employer's ability to prove acknowledgment of some policies is so important that employers sometimes choose to present them as stand-alone policies.

Before using this acknowledgment, employers should ensure their policies comply with applicable laws and do not violate or otherwise interfere with employees' rights. For example, employers should not maintain or implement policies that interfere with employees' **Section 7 rights** under the NLRA. For more information, see Standard Document, Stand-Alone Policy Acknowledgment: Drafting Note: General.

Employers using this policy as a stand-alone policy for their nonunionized employees should include the first alternative acknowledgment. However, employers using this policy as part of a larger handbook for nonunionized employees can use a single acknowledgment for the entire handbook (see Standard Document, Employee Handbook Acknowledgment).

Employers using this policy as a stand-alone policy for their unionized employees should include the second alternative acknowledgment. This alternative acknowledgment does not require a unionized employee to acknowledge the employer's right to modify or delete its provisions without notice or to terminate employment at will. The **National Labor Relations Board** (NLRB) may consider those statements evidence of a violation of an employer's duty to bargain with the employee's union before making changes to terms or conditions of employment under Sections 8(d) and 8(a)(5) of the NLRA (see *United Cerebral Palsy of N.Y.C.*, 347 N.L.R.B. 603 (2006)).

Employers using this policy as part of a larger handbook applicable to unionized employees can use a single acknowledgment for the entire handbook (see Standard Document, Unionized Employee Handbook Acknowledgment).

_____

Signature

_____

Printed Name

_____

Date]

APPENDIX

RECORD RETENTION SCHEDULE

Occasionally [COMPANY NAME] establishes retention or destruction schedules or procedures for specific categories of records. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Employees should give special consideration to the categories of documents listed in the record retention schedule below. Avoid retaining a record if there is no business reason for doing so, and consult with the Document Management Officer or Legal Department if unsure.

RECORD	RETENTION PERIOD
Personnel Records	
Benefits descriptions per employee	[Permanent/4 years]
Collective bargaining agreements	3 years
Donor records and acknowledgement letters	7 years
EEO-1 Reports (Employer Information Report)	Filed annually with the EEOC and the Department of Labor, Office of Federal Contract Compliance Programs, most recent kept on file
Employee applications and resumes	[4 years/1 year]
Employee benefit plans subject to ERISA (includes plans regarding health and dental insurance, 401K, long-term disability, and Form 5500)	6 years from when the record was required to be disclosed
Employee offer letters (and other documentation regarding hiring, promotion, demotion, transfer, lay-off, termination or selection for training)	1 year from date of making record or action involved, whichever is later, or 1 year from date of involuntary termination
Records relating to background checks on employees	5 years from when the background check is conducted
Employment contracts; employment and termination agreements	3 years from their last effective date
Employee records with information on pay rate or weekly compensation	3 years
Hazardous material exposures	Duration of employment + 30 years
I-9 Forms	[3 years after date of hire or 1 year after employment is terminated, whichever is later/3 years after date of hire]
Injury and Illness Incident Reports (OSHA Form 301) and related Annual Summaries (OSHA Form 300A); Logs of work-related injuries and illnesses (OSHA Form 300)	5 years following the end of the calendar year that these records cover
Supplemental record for each occupational injury or illness (OSHA Form 101); Log and Summary of Occupational Injuries and Illnesses (OSHA Form 200)	5 years following the year to which they relate
Job descriptions, performance goals and reviews; garnishment records	[Termination + 7 years/2 years]
Employee polygraph test records	3 years

Employee tax records	4 years from the date tax is due or paid
Medical exams required by law	Duration of employment + 30 years
Personnel or employment records [made or kept by a contractor or subcontractor with at least 150 employees or at least $150,000 in federal government contracts]	2 years from the date the record was made or personnel action was taken, whichever is later
Personnel or employment records [made or kept by a contractor or subcontractor with less than 150 employees or less than $150,000 in federal government contracts]	1 year from the date the record was made or personnel action was taken, whichever is later
Pension plan and retirement records	Permanent
Pre-employment tests and test results	1 year from date of personnel action
Salary schedules; ranges for each job description	2 years
Time reports	Termination + 3 years
Workers' compensation records	Duration of employment + 30 years
Written affirmative action program (AAP) and supporting documents	For immediately preceding AAP year, unless it was not then covered by the AAP year
Payroll Records	
Payroll registers (gross and net)	[Permanent/3 years from the last date of entry]
Federal procurement contract and related weekly payroll documents	4 years from completion of contract
Time cards; piece work tickets; wage rate tables; pay rates; work and time schedules; earnings records; records of additions to or deductions from wages; records on which wage computations are based	2 years
W-2 and W-4 Forms and Statements	As long as the document is in effect + 4 years
Corporate Records	
Articles of Incorporation, Bylaws, Corporate Seal	Permanent
Annual corporate filings and reports to secretary of state and attorney general	Permanent
Board policies, resolutions, meeting minutes, and committee meeting minutes	Permanent
Contracts	Permanent if current (7 years if expired)
Construction documents	Permanent
Emails (business related)	3 years
Fixed Asset Records	Permanent
IRS Form 1023 (Application for charitable and/or tax-exempt status)	Permanent
IRS Determination Letter	Permanent
Sales and purchase records	3 years
State sales tax exemption documents	Permanent
Records and reports on investigational drugs [for sponsors of clinical	2 years from when marketing application is approved for the drug. If

trials, usually pharmaceutical companies]	marketing application is not approved for the drug, retain until 2 years after shipment and delivery of the drug for investigational use is discontinued and FDA has been so notified
Resolutions	Permanent
Securities Records	
Audit and review workpapers	5 years from the end of the fiscal period in which the audit or review was concluded
Blotters or other records of original entry containing the itemized daily record of all purchases and sales of securities [applicable to broker-dealers]	6 years (for first 2 years, records must be kept in an easily accessible place)
Documents supporting management's assessment of internal controls over financial reporting	Permanent
List of clients that are covered associates and government entities	5 years (but not prior to September 13, 2010)
Order tickets for brokerage orders; customer complaints; compensation records	3 years (the first 2 years in an easily accessible place)
Original signature pages or other documents showing the signatures of certifying officers in SEC filings	5 years from date of filing
Records related to political contributions to officials and candidates and payments to state or local political parties and political action committees [applicable to investment advisers]	5 years (but not prior to September 13, 2010)
Records relevant to an audit or review, including memoranda, correspondence and other communications	7 years after conclusion of audit or review
Accounting and Finance	
Accounts Payable and Receivables ledgers and schedules	7 years
Annual audit reports and financial statements	Permanent
Annual plans and budgets	2 years
Bank statements, cancelled checks, deposit slips	7 years
Business expense records	7 years
Cash receipts	3 years
Check registers	Permanent
Electronic fund transfer documents	7 years
Employee expense reports	7 years
General ledgers	Permanent
Journal entries	7 years
Invoices	7 years
Petty cash vouchers	3 years
Tax Records	

Annual tax filing for the organization (IRS Form 990 in the US)	[Permanent/7 years]
Filings of fees paid to professionals (IRS Form 1099 in the US)	7 years
Payroll tax withholdings	7 years
Earnings records	7 years
Payroll tax returns	7 years
State unemployment tax records	Permanent
Legal and Insurance Records	
Appraisals	Permanent
Copyright registrations	Permanent
Environmental studies	Permanent
Insurance claims/ applications	Permanent
Insurance disbursements and denials	Permanent
Insurance contracts and policies (Directors and Officers, General Liability, Property, Workers' Compensation)	Permanent
Leases	6 years after expiration
Patents, patent applications, supporting documents	Permanent
Real estate documents (including loan and mortgage contracts, deeds)	Permanent
Stock and bond records	Permanent
Trademark registrations, evidence of use documents	Permanent
Warranties	Duration of warranty + 7 years

Note: ***Record Retention Schedule***

PRODUCTS

PLC Dispute Resolution, PLC US Federal Litigation, PLC US Labor and Employment, PLC US Law Department