



Take Yourself Seriously: Document Retention and Destruction Policies for Groups and Orgs

Rationale for Adoption of a Document Retention and Destruction Policy

Historically, dating to the pre-electronic records era, a principal rationale for a Document Retention and Destruction Policy ("DRD Policy"), has been to save space and save money by destroying paper documents which were no longer needed or required for an organization.

At the same time, another principal rationale for the DRD Policy was to ensure that the organization retained documents which could later be required for business or regulatory purposes. For example, maintaining tax documents in case of an audit or other investigation was a concern. Similarly, employment records were viewed as worthy of retention. Contract documents as well as those relating to ownership of organization assets also come into play in such a policy. Businesses in regulated industries may have other requirements.

In addition, document retention in case of litigation or governmental investigation became a consideration. In fact, particularly in light of developments in electronic (or e-) discovery, the proper maintenance and timely destruction of electronic (as well as paper) documents could save a great deal of money for an organization forced to search unwieldy and voluminous records in the face of discovery requests. At this time, compliance with law as it relates to litigation discovery and governmental investigations is another principal rationale for instituting and maintaining an appropriate DRD Policy and program.

IRS Form 990 instructs: "A document retention and destruction policy identifies the record retention responsibilities of staff, volunteers, board members, and outsiders for maintaining and documenting the storage and destruction of the organization's documents and records."

Considerations and Procedures for Implementation of a DRD Policy

A. First, discuss the ways in which documents are created or generated.

With respect to each employee or organizational function, are documents created which can be easily segregated from others, so that, when it comes time to destroy (or retain) those documents, they can be easily culled from the others for disposition? For example, on an employee-by-employee basis, are e-mails and other documents of a significantly non-sensitive nature so that they might be deleted, even in the face of a litigation hold with respect to other, more sensitive, documents? While this discussion will not necessarily dictate the provisions of the DRD Policy, it may go a long way toward achieving a major purpose of the Policy -- to conserve resources (such as, money and space) -- by identifying document streams in a way which will allow the DRD Policy to routinely provide for destruction of documents. Ideally, you will want to create and archive documents in a way that can readily identify and destroy documents with similar expirations.

B. Determine whether policies are already in place and, if so, whether they are worth retaining.

C. Determine how privacy laws will apply to documents and data from and with respect to employees and members/donors/volunteers.

The Policy and related procedures should provide or allow for complete compliance with such privacy laws. In addition, such procedures should be capable of audit and review on a regular basis.

D. Carefully think through the record retention responsibilities of staff, volunteers, board members, and outsiders (including partner orgs and coalition partners) for maintaining and documenting the storage and destruction of the organization's documents and records.

Although the IRS in its 990 instructions seems to imply that volunteers should have some responsibility, and, in fact, some special responsibility, with respect to such matters, the volunteers should have as little responsibility as possible. Anyone who is a volunteer (meaning that they are contributing their time, *gratis*) will think twice about continuing to volunteer if they are responsible for maintaining documents on their personal or business computers for some specified amount of time, for searching for documents on their computers and/or for destroying certain documents. These responsibilities should instead rest on management and staff.

E. Ensure that the policy includes standards for document integrity, including guidelines for handling electronic files, backup procedures, archiving of documents, and regular checkups of the reliability of the system. **Only include requirements which**

management knows will be met within the capabilities of the organization (if the org can't follow the policy, don't enact it). The worst thing that an organization can do is to adopt policies which it does not follow, since liability will then surely ensue.

- F.** Provide for one specific policy administrator (with assistants, if necessary) who will be responsible for administration of the policy.

Such individual's responsibilities should include periodic review of the policies for current relevance and compliance. If that administrator is not the ED/CEO, then the administrator should report to that person (since they are ultimately responsible for almost everything).

- G.** The policy must contain specific procedures for instituting a litigation hold where litigation, an audit or a government investigation is reasonably anticipated.

As indicated above, this is an area where liability could be significant if proper procedures are not instituted and followed.

- H.** Once the policy is adopted, it should be explained to employees to the extent that they are able to assist in its compliance.

- I.** The DRD Policy should be carefully explained to and adopted by the Board of Directors.

Prior to adoption, it should be determined where the policy should be placed in the organization's documentation. Alternatives may include, for example, in an employee manual, in the bylaws, in a board policies and procedures manual or as a stand-alone item. The manner in which the policy must or will be adopted – such as by the board of directors (recommended), by the members, or both – should also be determined.

- J.** In every case, the policy must be disseminated to all affected constituencies such as, for example, employees, directors, members and volunteers. Finally, the organization should only adopt policies which it is confident it can follow. It could well be worse to adopt a policy which is not followed than to have no policy at all.

Practice Pointers

- Document retention policies apply equally to documents saved in the cloud, on a server, or in a filing cabinet. If your nonprofit is using digital storage, make sure you have a back-up plan!
- While having a document retention policy gives staff the green light to toss certain documents (on a schedule, preferably), as you are creating a policy specifically for your nonprofit, think about whether there are certain types of documents or specific documents that for the sake of history, or institutional memory, should be maintained permanently.
- State laws relating to employment (such as those governing employment/payroll) vary state to state and often have implications for document retention policies.
- Nonprofits serving minor children may need to retain records relating to minor children at least until the child reaches majority age, plus the time allowed by the state statute of limitations for the child-now-adult to bring a claim against the nonprofit.
- Check with the professional advisor/accounting firm that prepares your nonprofit's annual returns to the IRS and ask what documents may be needed in the event of an IRS audit, and how long to retain them.
- Your nonprofit may want to include a preamble to its policy, emphasizing the connection between a document retention policy and the fiduciary duty of the board of directors. This language is from the Minnesota Council of Nonprofits, Principles and Practices for Nonprofit Excellence. "...The adoption of a document retention policy sets guidelines and facilitates directors' fulfillment of the duty of care, establishes transparency and ensures compliance."
- While it may not be obvious, email records are "documents" that should also be addressed in the nonprofit's document retention policy.

Specific Consideration for Certain Groups:

Sarbanes-Oxley Requirements

Section 802 (Criminal Penalties for Altering Documents) of the Sarbanes-Oxley Act (—SOXl) added Section 1519 to the federal criminal code, which provides:

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

SOX Section 1102 (Tampering with a Record or Otherwise Impeding an Official Proceeding) added a new subsection (c) to Section 1512 of the federal criminal code, which states:

(c) Whoever corruptly— (1) 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 (2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so, shall be fined under this title or imprisoned not more than 20 years, or both.

In addition to possible criminal liability, civil liability may result from the wrongful destruction of evidence, or —spoliation.!

If Litigation has already been filed against you (or you have initiated a suit against others)

Federal Rules of Civil Procedure

Among other things, Federal Rule of Civil Procedure (“FRCP”) 26(a)(1) requires a party to voluntarily provide a copy — or a description by category and location — of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment;

FRCP 26(b)(1) provides in pertinent part:

Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense — including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.

FRCP 37(e) states:

Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

Note that “good faith” is an element of this defense. Negligence, willfulness or gross negligence in dealing with these matters will result in penalties.

An organization becomes subject to a duty to preserve (or halt the destruction of) records once litigation, an audit or a government investigation is reasonably anticipated. *Zubulake v. UBS Warburg*, 220 F.R.D. 216 (S.D.N.Y. 2003).

At the same time, in order to comply with the preservation obligation, a company need not suspend the destruction of non-relevant records. Rather, parties should take steps to preserve the relevant information, what is sometimes known as a “litigation hold.” See *William T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Calif. 1984), where the court stated:

While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

Sample Document Retention and Destruction Policies

RECORD RETENTION AND DESTRUCTION POLICY (from Donors Forum—Lauren’s pick)

1) Purpose

The purpose of this Policy is to ensure that necessary records and documents of are adequately protected and maintained and to ensure that records that are no longer needed by or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of in

understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

2) Policy

This Policy represents the _____'s policy regarding the retention and disposal of records and the retention and disposal of electronic documents.

3) Administration

Attached as Appendix A is a Record Retention Schedule that is approved as the initial maintenance, retention and disposal schedule for physical records of _____ and the retention and disposal of electronic documents. The {Insert Title of Policy Administrator} (the "Administrator") is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. The Administrator is also authorized to: make modifications to the Record Retention Schedule from time to time to ensure that it is in compliance with local, state and federal laws and includes the appropriate document and record categories for _____; monitor local, state and federal laws affecting record retention; annually review the record retention and disposal program; and monitor compliance with this Policy.

4) Suspension of Record Disposal In Event of Litigation or Claims

In the event _____ is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning _____ or the commencement of any litigation against or concerning _____, such employee shall inform the Administrator and any further disposal of documents shall be suspended until such time as the Administrator, with the advice of counsel, determines otherwise. The Administrator shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.



5) Applicability

This Policy applies to all physical records generated in the course of _____'s operation, including both original documents and reproductions. It also applies to the electronic documents described above.

This Policy was approved by the Board of Directors of _____ on _____.

APPENDIX A - RECORD RETENTION SCHEDULE

The Record Retention Schedule is organized as follows:

SECTION TOPIC

- A. Accounting and Finance
- B. Contracts
- C. Corporate Records
- D. Correspondence and Internal Memoranda
- E. Electronic Documents
- F. Grant Records
- G. Insurance Records
- H. Legal Files and Papers
- I. Miscellaneous
- J. Payroll Documents
- K. Pension Documents
- L. Personnel Records
- M. Property Records
- N. Tax Records
- O. Contribution Records
- P. Programs & Services Records
- Q. Fiscal Sponsor Project Records

A. ACCOUNTING AND FINANCE

Record Type	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Annual Audit Reports and Financial Statements	Permanent
Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual Plans and Budgets	2 years
Bank Statements and Canceled Checks	7 years

Record Type	Retention Period
Employee Expense Reports	7 years
General Ledgers	Permanent
Interim Financial Statements	7 years
Notes Receivable ledgers and schedules	7 years
Investment Records	7 years after sale of investment
Credit card records (documents showing customer credit card number)	2 years

1. Credit card record retention and destruction

A credit card may be used to pay for the following products and services: .

All records showing customer credit card number must be locked in a desk drawer or a file cabinet when not in immediate use by staff.

If it is determined that information on a document, which contains credit card information, is necessary for retention beyond 2 years, then the credit card number will be cut out of the document.

B. CONTRACTS

Record Type	Retention Period
Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documentation)	7 years after expiration or termination

C. CORPORATE RECORDS

Record Type	Retention Period
Corporate Records (minute books, signed minutes of the Board and all committees, corporate seals, articles of incorporation, bylaws, annual corporate reports)	Permanent
Licenses and Permits	Permanent



D. CORRESPONDENCE AND INTERNAL MEMORANDA

General Principle: Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded *within two years*. Some examples include:
 - Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
 - Form letters that require no follow-up.
 - Letters of general inquiry and replies that complete a cycle of correspondence.
 - Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change).
 - Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
 - Chronological correspondence files.

Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

E. ELECTRONIC DOCUMENTS

1. **Electronic Mail:** Not all email needs to be retained, depending on the subject matter.
 - All e-mail—from internal or external sources—is to be deleted after 12 months.
 - Staff will strive to keep all but an insignificant minority of their e-mail related to business issues.
 - will archive e-mail for six months after the staff has deleted it, after which time the e-mail will be permanently deleted.
 - All business-related email should be downloaded to a service center or user directory on the server.
 - Staff will not store or transfer -related e-mail on non-work-related computers except as necessary or appropriate for purposes.
 - Staff will take care not to send confidential/proprietary information to outside sources.



- Staff with more than 500MB in their e-mail account will be unable to send or receive messages until the size of their account is reduced. Staff will be notified by _____ as their account size approaches 500 MB.
 - Any e-mail staff deems vital to the performance of their job should be copied to the staff's H: drive folder, and printed and stored in the employee's workspace.
2. Electronic Documents: including Microsoft Office Suite and PDF files. Retention also depends on the subject matter.
- **PDF documents** – The length of time that a PDF file should be retained should be based upon the content of the file and the category under the various sections of this policy. The maximum period that a PDF file should be retained is 6 years. PDF files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace.
 - **Text/formatted files** - Staff will conduct annual reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those they consider unnecessary or outdated. After five years, all text files will be deleted from the network and the staff's desktop/laptop. Text/formatted files the staff deems vital to the performance of their job should be printed and stored in the staff's workspace.
3. **Web Page Files: Internet Cookies**
- All workstations: Internet Explorer should be scheduled to delete Internet cookies once per month.

_____ does not automatically delete electronic files beyond the dates specified in this Policy. It is the responsibility of all staff to adhere to the guidelines specified in this policy.

Each day _____ will run a tape backup copy of all electronic files (including email) on _____'s servers, as specified in the _____ Disaster Recovery Plan. This backup tape is a safeguard to retrieve lost information within a one-year retrieval period should documents on the network experience problems. The tape backup copy is considered a safeguard for the record retention system of _____, but is not considered an official repository of _____ records. All monthly and yearly tapes are stored offsite according to _____'s Disaster Recovery Policy.

In certain cases a document will be maintained in both paper and electronic form. In such cases the official document will be the electronic document.

F. GRANT RECORDS

Record Type	Retention Period
Original grant proposal	7 years after completion of grant period
Grant agreement and subsequent modifications, if applicable	7 years after completion of grant period
All requested IRS/grantee correspondence including determination letters and "no change" in exempt status letters	7 years after completion of grant period

Record Type	Retention Period
Final grantee reports, both financial and narrative	7 years after completion of grant period
All evidence of returned grant funds	7 years after completion of grant period
All pertinent formal correspondence including opinion letters of counsel	7 years after completion of grant period
Report assessment forms	7 years after completion of grant period
Documentation relating to grantee evidence of invoices and matching or challenge grants that would support grantee compliance with the grant agreement	7 years after completion of grant period
Pre-grant inquiry forms and other documentation for expenditure responsibility grants	7 years after completion of grant period
Grantee work product produced with the grant funds	7 years after completion of grant period

G. INSURANCE RECORDS

Record Type	Retention Period
Annual Loss Summaries	10 years
Audits and Adjustments	3 years after final adjustment
Certificates Issued to	Permanent
Claims Files (including correspondence, medical records, injury documentation, etc.)	Permanent
Group Insurance Plans - Active Employees	Until Plan is amended or terminated
Group Insurance Plans – Retirees	Permanent or until 6 years after death of last eligible participant
Inspections	3 years
Insurance Policies (including expired policies)	Permanent
Journal Entry Support Data	7 years

**Record Type****Retention Period**

Loss Runs

10 years

Releases and Settlements

25 years

H. LEGAL FILES AND PAPERS

Record Type	Retention Period
Legal Memoranda and Opinions (including all subject matter files)	7 years after close of matter
Litigation Files	1 year after expiration of appeals or time for filing appeals
Court Orders	Permanent
Requests for Departure from Records Retention Plan	10 years

I. MISCELLANEOUS

Record Type	Retention Period
Consultant's Reports	2 years
Material of Historical Value (including pictures, publications)	Permanent
Policy and Procedures Manuals – Original	Current version with revision history
Policy and Procedures Manuals - Copies	Retain current version only
Annual Reports	Permanent

J. PAYROLL DOCUMENTS

Record Type	Retention Period
Employee Deduction Authorizations	4 years after termination
Payroll Deductions	Termination + 7 years
W-2 and W-4 Forms	Termination + 7 years
Garnishments, Assignments, Attachments	Termination + 7 years
Labor Distribution Cost Records	7 years
Payroll Registers (gross and net)	7 years



Record Type	Retention Period
Time Cards/Sheets	2 years
Unclaimed Wage Records	6 years

K. PENSION DOCUMENTS AND SUPPORTING EMPLOYEE DATA

General Principle: Pension documents and supporting employee data shall be kept in such a manner that Donors Forum can establish at all times whether or not any pension is payable to any person and if so the amount of such pension.

Record Type	Retention Period
Retirement and Pension Records	Permanent

L. PERSONNEL RECORDS

Record Type	Retention Period
Commissions/Bonuses/Incentives/Awards	7 years
EEO- I /EEO-2 - Employer Information Reports	2 years after superseded or filing (whichever is longer)
Employee Earnings Records	Separation + 7 years
Employee Handbooks	1 copy kept permanently
Employee Medical Records	Separation + 6 years
Employee Personnel Records (including individual attendance records, application forms, job or status change records, performance evaluations, termination papers, withholding information, garnishments, test results, training and qualification records)	6 years after separation
Employment Contracts – Individual	7 years after separation
Employment Records - Correspondence with Employment Agencies and Advertisements for Job Openings	3 years from date of hiring decision

Record Type	Retention Period
Employment Records - All Non-Hired Applicants (including all applications and resumes - whether solicited or unsolicited, results of post-offer, pre-employment physicals, results of background investigations, if any, related correspondence)	2-4 years (4 years if file contains any correspondence which might be construed as an offer)
Job Descriptions	3 years after superseded
Personnel Count Records	3 years
Forms I-9	3 years after hiring, or 1 year after separation if later

M. PROPERTY RECORDS

Record Type	Retention Period
Correspondence, Property Deeds, Assessments, Licenses, Rights of Way	Permanent
Original Purchase/Sale/Lease Agreement	Permanent
Property Insurance Policies	Permanent

N. TAX RECORDS

General Principle: Donors Forum must keep books of account or records as are sufficient to establish amount of gross income, deductions, credits, or other matters required to be shown in any such return.

These documents and records shall be kept for as long as the contents thereof may become material in the administration of federal, state, and local income, franchise, and property tax laws.

Record Type	Retention Period
Tax-Exemption Documents and Related Correspondence	Permanent
IRS Rulings	Permanent
Excise Tax Records	7 years
Payroll Tax Records	7 years



Record Type	Retention Period
Tax Bills, Receipts, Statements	7 years
Tax Returns - Income, Franchise, Property	Permanent
Tax Workpaper Packages - Originals	7 years
Sales/Use Tax Records	7 years
Annual Information Returns - Federal and State	Permanent
IRS or other Government Audit Records	Permanent

O. CONTRIBUTION RECORDS

Record Type	Retention Period
Records of Contributions	Permanent
's or other documents evidencing terms of gifts	Permanent

P. PROGRAM AND SERVICE RECORDS

Record Type	Retention Period
	7 years
convenings	Permanent (1 copy only)
Research & Publications	Permanent (1 copy only)

Q. FISCAL SPONSOR PROJECT RECORDS

Record Type	Retention Period
Sponsorship agreements	Permanent

DOCUMENT RETENTION AND DESTRUCTION POLICY

1. Policy and Purposes

This Policy represents the policy of _____ (the “organization”) with respect to the retention and destruction of documents and other records, both in hard copy and electronic media (which may merely be referred to as “documents” in this Policy). Purposes of the Policy include (a) retention and maintenance of documents necessary for the proper functioning of the organization as well as to comply with applicable legal requirements; (b) destruction of documents which no longer need to be retained; and (c) guidance for the Board of Directors, officers, staff and other constituencies with respect to their responsibilities concerning document retention and destruction. Notwithstanding the foregoing, the organization reserves the right to revise or revoke this Policy at any time.

2. Administration

2.1 Responsibilities of the Administrator. The organization’s _____ [CEO, President, Executive Vice President, Vice President for ___, etc.] shall be the administrator (“Administrator”) in charge of the administration of this Policy. The Administrator’s responsibilities shall include supervising and coordinating the retention and destruction of documents pursuant to this Policy and particularly the Document Retention Schedule included below. The Administrator shall also be responsible for documenting the actions taken to maintain and/or destroy organization documents and retaining such documentation. The Administrator may also modify the Document Retention Schedule from time to time as necessary to comply with law and/or to include additional or revised document categories as may be appropriate to reflect organizational policies and procedures. The Administrator is also authorized to periodically review this Policy and Policy compliance with legal counsel and to report to the Board of Directors as to compliance. The Administrator may also appoint one or more assistants to assist in carrying out the Administrator’s responsibilities, with the Administrator, however, retaining ultimate responsibility for administration of this Policy.

2.2 Responsibilities of Constituencies. This Policy also relates to the responsibilities of board members, staff, volunteers and outsiders (including coalition partners) with respect to maintaining and documenting the storage and destruction of the organization’s documents. The Administrator shall report to the Board of Directors (the board members acting as a body), which maintains the ultimate direction of management. The organization’s staff shall be familiar with this Policy, shall act in accordance therewith, and shall assist the Administrator, as requested, in implementing it. The responsibility of volunteers with respect to this Policy shall be to produce specifically identified documents upon request of management, if the volunteer still retains such documents. In that regard, after each project in which a volunteer has been involved, or each term which the volunteer has served, it shall be the responsibility of the Administrator to confirm whatever types of documents the volunteer retained and to request any such documents which the Administrator feels will be necessary for retention by the organization (not by the volunteer). Outsiders may include vendors, coalition partners or other service providers. Depending upon the sensitivity of the documents involved with the particular outsider relationship, the organization, through the Administrator, shall share this Policy with the outsider, requesting compliance. In particular instances, the Administrator may require that the contract with the outsider specify the particular responsibilities of the outsider with respect to this Policy.

3. Suspension of Document Destruction; Compliance. The organization becomes subject to a duty to preserve (or halt the destruction of) documents once litigation, an audit or a government investigation is reasonably anticipated. Further, federal law imposes criminal liability (with fines and/or imprisonment for not more than 20 years) upon whomever “knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States ... or in relation to or contemplation of any such matter or case.” Therefore, if the Administrator becomes aware that litigation, a governmental audit or a government investigation has been instituted, or is reasonably anticipated or contemplated, the Administrator shall immediately order a halt to all document destruction under this Policy, communicating the order to all affected constituencies in writing. The Administrator may thereafter amend or rescind the order only after conferring with legal counsel. If any board member or staff member becomes aware that litigation, a governmental audit or a government investigation has been instituted, or is reasonably anticipated or contemplated, with respect to the organization, and they are not sure whether the Administrator is aware of it, they shall make the Administrator aware of it. Failure to comply with this Policy, including, particularly, disobeying any destruction halt order, could result in possible civil or criminal sanctions. In addition, for staff, it could lead to disciplinary action including possible termination.

4. Electronic Documents; Document Integrity. Documents in electronic format shall be maintained just as hard copy or paper documents are, in accordance with the Document Retention Schedule. Due to the fact that the integrity of electronic documents, whether with respect to the ease of alteration or deletion, or otherwise, may come into question, the Administrator shall attempt to establish standards for document integrity, including guidelines for handling electronic files, backup procedures, archiving of documents, and regular checkups of the reliability of the system; provided, that such standards shall only be implemented to the extent that they are reasonably attainable considering the resources and other priorities of the organization.



5. Privacy. It shall be the responsibility of the Administrator, after consultation with counsel, to determine how privacy laws will apply to the organization's documents from and with respect to employees and other constituencies; to establish reasonable procedures for compliance with such privacy laws; and to allow for their audit and review on a regular basis.

6. Emergency Planning. Documents shall be stored in a safe and accessible manner. Documents which are necessary for the continued operation of the organization in the case of an emergency shall be regularly duplicated or backed up and maintained in an off-site location. The Administrator shall develop reasonable procedures for document retention in the case of an emergency.

7. Document Creation and Generation. The Administrator shall discuss with staff the ways in which documents are created or generated. With respect to each employee or organizational function, the Administrator shall attempt to determine whether documents are created which can be easily segregated from others, so that, when it comes time to destroy (or retain) those documents, they can be easily culled from the others for disposition. For example, on an employee-by-employee basis, are e-mails and other documents of a significantly non-sensitive nature so that they might be deleted, even in the face of a litigation hold with respect to other, more sensitive, documents? This dialogue may help in achieving a major purpose of the Policy -- to conserve resources -- by identifying document streams in a way that will allow the Policy to routinely provide for destruction of documents. Ideally, the organization will create and archive documents in a way that can readily identify and destroy documents with similar expirations.

8. Document Retention Schedule. [Periods are suggested but are not necessarily a substitute for your (or your attorney's) own research and determination as to appropriate periods.]

Document Type	Retention Period
Accounting and Finance	
Accounts Payable	7-10 years
Accounts Receivable	7-10 years
Annual Financial Statements and Audit Reports	Permanent
Bank Statements, Reconciliations & Deposit Slips	7 years
Canceled Checks – routine	7 years
Canceled Checks – special, such as loan repayment	Permanent
Credit Card Receipts	3 years
Employee/Business Expense Reports/Documents	7 years
General Ledger	Permanent
Interim Financial Statements	7 years
Contributions/Gifts/Grants	
Contribution Records	Permanent
Documents Evidencing Terms of Gifts	Permanent
Grant Records	7 yrs after end of grant period
Corporate and Exemption	
Articles of Incorporation and Amendments	Permanent
Bylaws and Amendments	Permanent
Minute Books, including Board & Committee Minutes	Permanent
Annual Reports to Attorney General & Secretary of State	Permanent
Other Corporate Filings	Permanent
IRS Exemption Application (Form 1023 or 1024)	Permanent
IRS Exemption Determination Letter	Permanent
State Exemption Application (if applicable)	Permanent
State Exemption Determination Letter (if applicable)	Permanent
Licenses and Permits	Permanent
Employer Identification (EIN) Designation	Permanent

Correspondence and Internal Memoranda

Hard copy correspondence and internal memoranda relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate.

Hard copy correspondence and internal memoranda relating to routine matters with no lasting significance	Two years
--	-----------

Correspondence and internal memoranda important to the organization or having lasting significance	Permanent, subject to review
--	------------------------------

Electronic Mail (E-mail) to or from the organization

Electronic mail (e-mails) relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate, but may be retained in hard copy form with the document to which they relate.

The AICPA Audit Committee Toolkit: Not-for-Profit Organizations

E-mails considered important to the organization or of lasting significance should be printed and stored in a central repository .

Permanent, subject to review

E-mails not included in either of the above categories

12 months (this can be shorter if desired)

Electronically Stored Documents

Electronically stored documents (e.g., in pdf, text or other electronic format) comprising or relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document which they comprise or to which they relate, but may be retained in hard copy form (unless the electronic aspect is of significance).

Electronically stored documents considered important to the organization or of lasting significance should be printed and stored in a central repository (unless the electronic aspect is of significance).

Permanent, subject to review

Electronically stored documents not included in either of the above categories

Two years

Employment, Personnel and Pension

Personnel Records

10 yrs after employment ends

Employee contracts

10 yrs after termination

Retirement and pension records

Permanent

Insurance

Property, D&O, Workers' Compensation and

General Liability Insurance Policies

Permanent

Insurance Claims Records

Permanent

Legal and Contracts

Contracts, related correspondence and other supporting documentation

10 yrs after termination

Legal correspondence

Permanent

Management and Miscellaneous

Strategic Plans

7 years after expiration

Disaster Recovery Plan

7 years after replacement

Policies and Procedures Manual

Current version with revision history

Property – Real, Personal and Intellectual

Property deeds and purchase/sale agreements

Permanent

Property Tax

Permanent

Real Property Leases

Permanent

Personal Property Leases

10 years after termination

Trademarks, Copyrights and Patents

Permanent

Tax

Tax exemption documents & correspondence

Permanent

IRS Rulings

Permanent

Annual information returns – federal & state

Permanent

Tax returns

Permanent

The Document Retention and Destruction Policy identifies the record retention responsibilities of staff, volunteers, members of the board of directors, and outsiders for maintaining and documenting the storage and destruction of the organization's documents and records.



The organization's staff, volunteers, members of the board of directors, committee members and outsiders (independent contractors via agreements with them) are required to honor the following rules:

- a. Paper or electronic documents indicated under the terms for retention in the following section will be transferred and maintained by (fill in the blank based on the organization's practices);
- b. All other paper documents will be destroyed after three years;
- c. All other electronic documents will be deleted from all individual computers, data bases, networks, and back-up storage after one year;
- d. No paper or electronic documents will be destroyed or deleted if pertinent to any ongoing or anticipated government investigation or proceeding or private litigation (check with legal counsel or the human resources department for any current or foreseen litigation if employees have not been notified); and
- e. No paper or electronic documents will be destroyed or deleted as required to comply with government auditing standards (add specific standards here if relevant)


Record Retention

The following table* indicates the minimum requirements and is provided as guidance to customize in determining your organization's document retention policy. Because statutes of limitations and state and government agency requirements vary from state to state, each organization should carefully consider its requirements and consult with legal counsel before adopting a Document Retention and Destruction Policy. In addition, federal awards and other government grants may provide for a longer period than is required by other statutory requirements.

* Adapted from National Council of Nonprofits.

Type of Document	Minimum Requirement
Accounts payable ledgers and schedules	7 years
Audit reports	Permanently
Bank reconciliations	2 years
Bank statements	3 years
Checks (for important payments and purchases)	Permanently
Contracts, mortgages, notes, and leases (expired)	7 years
Contracts (still in effect)	Contract period
Correspondence (general)	2 years
Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2 years
Deeds, mortgages, and bills of sale	Permanently
Depreciation schedules	Permanently
Duplicate deposit slips	2 years
Employment applications	3 years
Expense analyses/expense distribution schedules	7 years
Year-end financial statements	Permanently
Insurance records, current accident reports, claims, policies, and so on (active and expired)	Permanently
Internal audit reports	3 years
Inventory records for products, materials, and supplies	3 years
Invoices (to customers, from vendors)	7 years
Minute books, bylaws, and charter	Permanently
Patents and related papers	Permanently
Payroll records and summaries	7 years
Personnel files (terminated employees)	7 years
Retirement and pension records	Permanently
Tax returns and worksheets	Permanently
Timesheets	7 years
Trademark registrations and copyrights	Permanently
Withholding tax statements	7 years

Resources

 National Council of Nonprofits www.councilofnonprofits.org

■ Guide to Record Retention Requirements in the Code of Federal Regulations: Contact the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402-9325 or from CCH, Inc. at www.onlinestore.cch.com

