



**RECORDS RETENTION
AND
DISPOSITION GUIDELINES**

**Prepared by the Collaborative Electronic Records Project
Rockefeller Archive Center
Revised November 2008**

This document may be freely used and modified by any non-profit organization.

TABLE OF CONTENTS

Introduction	3
How Long to Keep Records	4
Categorizing Information	7
Keeping Records Electronically	8
Storing Records	9
Destroying Records	10
Certificate of Destruction	12
Resources	13

RECORDS RETENTION AND DISPOSITION GUIDELINES

Introduction

Non-profit organizations, like for-profit ones, need to retain certain records beyond current use needs, according to regulatory, legal, financial, and operational requirements. Which records to keep and for how long may vary from organization to organization. Whether a record is in paper or electronic format does not determine its value or retention period; its content is the key factor. Records referenced in this schedule include paper, electronic (including e-mail), and voicemail regardless of whether the record is stored in traditional containers such as file cabinets and boxes, or on a network server, desktop, laptop, handheld, or other device with text or instant messaging capability. The following schedule is merely a sample of a typical non-profit's need for retaining records and reflects the minimum suggested retention period. When a record is no longer needed or required, it should be disposed of properly in order to ensure that the data truly is no longer recoverable. Electronic records that are to be retained permanently must be pro-actively managed if the information is to remain viable, authentic, and accessible.

Several Federal and State laws contain recordkeeping requirements, including the Americans with Disabilities Act (ADA), Age Discrimination in Employment Act (ADEA), Equal Pay Act, Executive Order 11246, Family and Medical Leave Act (FMLA), Fair Labor Standards Act (FLSA), Health Insurance Portability and Accountability Act (HIPPA), Title VII of the Civil Rights Act of 1964, Immigration Reform and Control Act (IRCA), Occupational Safety and Health Act (OSHA), Employee Retirement Income Security Act (ERISA), and the Vietnam Era Veterans' Readjustment Assistance Act of 1974. Each organization should consult its own attorney and accountant, as well as federal and state regulators, for expert advice on records retention. Records management guidelines and schedules should be reviewed at least annually to be sure they comply with current requirements. For additional guidance, see your organization's Records Management Guidelines.¹

¹ If your organization has no formal guidelines, you may use guidance documents prepared by the Collaborative Electronic Records Project: <<http://siarchives.si.edu/cerp/cerpindex.htm>>.

How Long to Keep Records ²

<u>Document Content</u>	<u>Minimum Retention</u> ³
Accident reports and claims (settled cases)	7 years
Accounts receivable & payable ledgers & schedules	7 years
Affirmative Action Plan	1 year after plan expires
Articles of Incorporation, charter, bylaws, minutes, and other incorporation records	Permanently
Audit reports	Permanently
Bank statements, deposit records, electronic funds transfer evidence, cancelled checks, reconciliation	7 years
Bylaws and charter	Permanently
Chart of accounts	Permanently
Checks for important payments and purchases	Permanently
Contracts, mortgages, notes and leases (expired)	7 years
Contracts (still in effect)	Until 7 years after expiration
Copyright, trademark, patent registrations	Permanently
Correspondence, administrative (pertaining to formulation, planning, implementation, interpretation, modification, redefinition of programs, services, projects and the regulations, policies, and procedures that govern them)	3 years
Correspondence, general (Non-administrative incoming/outgoing and internal correspondence pertaining to or arising from the routine operations of the policies, programs, services, or projects)	1 year

² Records required in connection with a lawsuit or potential legal action must be retained until litigation is settled and the appeal time expires.

³ This schedule draws heavily from the National Council of Nonprofit Associations example: <<http://www.ncna.org>>.

Correspondence, legal and important matters	Permanently
Correspondence with customers and vendors	2 years
Deeds, mortgages, bills of sale	Permanently
Depreciation schedules	Permanently
Donations	7 years
Employee demographics records ⁴	3 years
Employee discrimination reports (EEOC, ADA, etc.)	Permanently
Employment applications ⁵	3 years from record creation or personnel action
Expense Analyses & distribution schedules	7 years
Financial Statements, year-end	Permanently
Garnishments	7 years
General ledgers, year-end trial balance, journals	Permanently
Grants, un-funded	1 year
Grants, funded	7 years after closure
I-9s*	3 years after hire date
Insurance policies	3 years after expiration
Insurance records, accident reports, claims, etc.	Permanently
Internal audit reports	3 years
Invoices (to customers, from vendors)	7 years

⁴ Davis-Bacon Act, Service Contract Act, & Walsh-Healy Public Contracts Act

⁵ Depending on the number of employees, employers must retain applications & other personnel records relating to hires, rehires, tests, promotions, transfers, demotions, selection for training, layoff, recall, termination or discharge (Civil Rights Act of 1964, Title VII, ADA, ADEA).

Inventory records	7 years
Journals	Permanently
Loan documents and notes	Permanently
Material Safety Data Sheets	Permanently
Mission Statements, Strategic plans	Permanently
Notes receivable ledgers and schedules	7 years
Organization charts	Permanently
OSHA logs*	5 years
OSHA records related to medical exams	30 years after termination
Patents and related papers	Permanently
Payroll records & summaries including expense reports and records related to employee leave* (Equal Pay Act, FLSA)	7 years
Personnel files, terminated employees	7 years after termination
Petty cash vouchers	3 years
Polygraph test results and records* (Employee Polygraph Protection Act)	3 years
Program and/or project files (not grant specific)	Permanently
Property appraisals by outside appraisers	Permanently
Property records including costs, depreciation schedules	Permanently
Property blueprints and facility utility diagrams	Permanently (or until property is sold)
Purchase orders	7 years
Retirement and pension records including Summary Plan Descriptions* (ERISA)	Permanently

Sales records	7 years
Stock and bond certificates (cancelled)	7 years
Tax returns and worksheets	Permanently
Timesheets, books, cards	7 years
Training manuals	Permanently
Vouchers for payments to vendors, employees, etc. (includes employee/officer travel & entertainment expense reimbursements)	7 years
Withholding tax statements* (FICA, FUTA, Federal Income)	7 years
Workers compensation documentation	10 years after 1 st closure

* If, while completing the Affirmative Action Plan, an "adverse impact" is discovered, then the records must be maintained until two years after the adverse impact is eliminated.

** Medical records related to a leave granted under the Family and Medical Leave Act (FMLA) must be maintained for three years.

Categorizing Information

Because the list above is not all-inclusive, you may need to determine whether a particular item is considered a record, and thus, subject to a records retention and disposition schedule. Some of the characteristics of a record are:

- Contains legal or regulatory compliance information⁶
- Evidences a transaction
- Identifies participants in business activities or who had knowledge of an event
- Proves a business-related event or activity occurred or did not occur

It may be useful when making retention decisions to sort records into three categories – enduring value, limited value, and no value – and establish time periods to keep each group regardless of their form (paper or electronic).

Category 1 – Records with enduring value

Retain Permanently (Examples, not all inclusive):

- Agendas and meeting minutes
- Appointment calendars of executives
- Correspondence related to official business communications at the executive level to and from others inside and outside the organization

⁶ Charlene Brownlee, and Melissa Cozart, "The Challenge of Electronic Records," *The Corporate Counselor, Law Journal Newsletters*, Vol. 20, No. 1 (June 2005) <<http://www.ljnonline.com/>>.

- Distribution list member names and e-mail addresses for each list
- Documentation of departmental and organizational decisions and operations
- E-mail transmittals – messages containing no substantive information that are sent only to provide attachments. Because the legal authenticity of an e-mail requires retention of its metadata (the transmission data), transmittals may supply a key part of the record.
- Grant proposals, approvals, reports
- Policy, program, and procedure directives

Category 2 – Records with limited value (Examples, not all inclusive. NOTE: Category 2 does not apply to records documenting essential organization, staffing, and procedures; see Category 1.)

Retain 3 years unless required longer for legal or regulatory purposes

- Budget records
- Day-to-day administration
- Facsimile machine logs
- Office services and equipment requests and receipts
- Supply orders and receipts
- Travel itineraries
- Utilities records

Category 3 – Records of little or no long-term value (Examples, not all inclusive)

Retain: 0-30 days or until no longer needed for reference

- Calendars (except for key executives)
- Copies of documents when the holder is not the official record keeper, sender, or primary addressee
- Copies of publications or other published reference materials
- Drafts, except for mission critical documents, program and policy changes, or original creative, artistic, and scientific works
- Informational, e.g. holiday closings, charitable drives, notifications of meetings
- Junk and SPAM mail, whether received via e-mail, fax, or traditional mail
- Messages to/from distribution lists (e.g. ListSrvs)
- Personal correspondence, e-mail, text messages, etc.
- Routine requests for information or publications and replies
- Scheduling of work assignments, work-related trips and visits
- Suspense files or 'to-do' and task lists that serve as a reminder that an action is required or a reply expected on a given date

Keeping Records Electronically

As a best practice measure to minimize potential loss of information, whether from disaster, human error, or other causes, all electronic records should be copied with one copy stored in a separate locale and one maintained in house. Preferred removable media are archival quality, gold CDs or DVDs. Keep in mind that even though an

archival quality optical disk may last over 100 years, the capability of reading it or accessing the data may be long gone. Both the Records Manager and IT manager should set up calendar reminders to migrate data from older media and formats at regular intervals to be sure the records remain viable for the required period of time. The current consensus is to test for degradation, refresh media, and migrate data every 5 years. The preferred formats are XML for born-digital records, PDF/A for text documents, and TIFF for images.

Migration decisions should consider the possibility of metadata loss or alteration; keyword search capability; the inability to annotate files; the necessity to maintain operating systems and software that supports original file formats; and the difficulty in tracing file users and dates.⁷ The terms, on-line, near-line, and off-line retention, are unique to electronic records, and refer to the type of storage media, **not** to the length of time the information in a particular record should be retained. The Records Manager and IT Manager should collaborate to decide which type of storage is appropriate for each category of record.

On-line retention period: usually refers to retaining data on magnetic disks for disaster recovery purposes, generally 1 week to 3 months.

Near-line retention period: data may remain on-site but on removable media such as CDs. Depending on the type of information contained, the records may be Category 1, 2, or 3. In the case of Category 1, Records with Enduring Value, the data may need to be migrated periodically to avoid loss of information from deteriorating media.

Off-line retention period: data may be stored off-site, typically on magnetic tapes. Like near-line retention, records in Category 1, Records with Enduring Value, should be transferred regularly to more permanent, stable media.⁸

Storing Records

Both the original digital records and the copies should be archived with each clearly identified and properly stored in an area with proper environmental controls.⁹ Originals may be kept segregated on a dedicated, non-networked server (recommended) in a secure space, or on removable media, or placed in a digital repository such as DSpace or Fedora, all with access limited to authorized Archivists. Originals or copies on CDs and DVDs should be stored in archival CD/DVD cases or Tyvek envelopes

⁷ Mary Mack, "Native File Review: Simplifying Electronic Discovery?" in *Law Journal Newsletters Legal Tech Newsletter*, Vol. 23, No. 2 (May 2005) <<http://www.ljonline.com/alm?It>>.

⁸ David O. Stephens and Roderick C. Wallace, *Electronic Records Retention: New Strategies for Data Life Cycle Management*, Lenexa, KS: ARMA International, 2003.

⁹ See "Care and Handling of CDs and DVDs – A Guide for Librarians and Archivists" by Fred Byers, NIST Special Publication 500-252, Oct. 2003 <http://www.itl.nist.gov/div895/carefordisc/>.

inside acid-free CD/DVD boxes. CD/DVD cases should be of inert polyester that does not release potentially harmful chemicals. Whether in cases or boxes, store the CD/DVDs vertically. Do not write directly on CD/DVDs unless using an archival soft tip pen and then write only on the clear center hub of the top side. Do not apply labels to optical media. Alternatively, identifying information may be written on the Tyvek envelope fold-over tab, using an archival soft tip pen.

Destroying Records

When a record is no longer required to be kept, it should be properly destroyed and the destruction should be documented. A sample Certificate of Records Destruction form is attached. For example, information entered on the form could be:

<u>Record Category</u>	<u>Format/Media</u>	<u>Date Range</u>	<u>Method</u>
Vouchers	paper	1960-1987	Shredder
Council Meetings	audio tape	1990-1991	Degaussing
Press release drafts	Word/CD	1990-1995	CD shredder
E-mail	mbox/server	1999-2001	Sanitized

Deleting data and emptying the “recycle” folder or “trash” bin from electronic storage media such as CDs, hard drives, tapes, etc. does not permanently destroy the information. Some printers and photocopiers with document memory capability may require data cleaning also before sale or disposal. If data is not sensitive or private, simply overwriting the information may be adequate.¹⁰ If computers and media are going to be reused or de-commissioned, they must be properly cleaned in order to prevent unauthorized retrieval and use of information, especially if that data includes privacy or security-related material such as personnel records, financial data, or employee health information.

To completely remove data or prevent its retrieval, the following methods should be used.

- ▶ Hard drives, USB or flash drives, and other plug-in type devices: Sanitize by running special software programs or following the manufacturer’s instructions for full chip erasure. For Windows operating systems, Active Eraser is one product that erases files and hard drives. It is available at <http://www.active-eraser.com/features.htm>. Another is Eraser by Tolvanen at <http://www.tolvanen.com/eraser/>. Macintosh operating systems will need a third-party utility such as Jiiva AutoScrubber (<http://www.jiiva.com/>) for version 10.2 file deletion and Jiiva SuperScrubber for hard drives. Versions 10.3 and 10.4 have built in Secure Empty Trash options; however, 10.3 also needs a third-party utility such as JiivaSuperScrubber for hard drives. Version 10.4 also requires Apple Disk Utility (Zero all data, 7- and 35-Pass Erase) for empty space

¹⁰ Overwriting is the process of writing patterns of data on top of the data stored on a magnetic medium in order to obscure the previously written data.

deletion and hard drive cleaning. If the drive is no longer operational, cables should be cut and the drive disassembled. Its platters should be damaged by drilling holes, hammering, or cutting with metal snips.

- ▶ Personal Digital Assistants (PDAs), Blackberry, etc.:

Clean data according to manufacturer's instructions and reset to factory defaults. Remove batteries for several hours. Alternatively, wrap securely to prevent flying particles and hammer until the internal parts are destroyed.

- ▶ Removable media:

Special shredders are available that can shred optical media (CDs, DVDs, etc.). Diskettes or other media not suitable for shredding should be disassembled and the media mutilated by puncturing, cutting, or sanding.

- ▶ Magnetic tape:

Degaussing¹¹ tailored for the type of tape and with proper coercivity.¹² Alternatively, incineration, pulverization, or shredding may be used. If the data sanitizing process is contracted to an outside party, the vendor should sign an agreement stating that their practices conform to or exceed the guidelines stated here.

¹¹ Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtually zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable.

¹² Coercivity specifies the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The coercivity strength of an applied magnetic field determines which type of degausser may be applied to a particular type of magnetic material.

CERTIFICATE OF RECORDS DESTRUCTION

I, _____, acting on behalf of

(Organization Name)

hereby certify that the following records were destroyed according to the Records Retention and Disposition Guidelines.

Collection/Record Group/Series: _____

Record Category (correspondence, etc.): _____

Format (mbox, Word, etc.) _____

Date Range: _____

Type media or, if hard drive, enter serial #: _____

Method: _____

Location of Disposal: _____

Signature: _____ Date: _____

Title: _____

Authorized by _____ Title: _____

Resources

Brownlee, Charlene and Melissa Cozart. "The Challenge of Electronic Records." *The Corporate Counselor, Law Journal Newsletters*, Vol. 20, No. 1 (June 2005).

<<http://www.ljnonline.com/>>.

Byers, Fred. "Care and Handling of CDs and DVDs – A Guide for Librarians and Archivists." NIST Special Publication 500-252, Oct. 2003

<http://www.itl.nist.gov/div895/carefordisc/>.

Collaborative Electronic Records Project. <<http://siarchives.si.edu/cerp/cerpindex.htm>>.

Dollar, Charles. *Authentic Electronic Records: Strategies for Long-Term Access*. Chicago: Cohasset Associates, Inc., 2002.

Dorothy A. Johnson Center for Philanthropy & Nonprofit Leadership, Grand Valley State University. "The Nonprofit Good Practice Guide."

<<http://www.auxillium.com/records.shtml>>.

Equality State Policy Center, Casper, WY. "Guidelines for Records Retention for Non-Profit Organizations".

<http://www.equalitystate.org/ESPC%20Website%20Generic%20Pages/workprogramfolder/Non%20profit%20files/w31aug01.html>.

Hunter, Gregory S. *Preserving Digital Information, A How-To-Do-It Manual for Librarians*. New York: Neal-Schuman Publishers, Inc., 2000.

Kissel, Richard, et al. "Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology." NIST Special Publication 800-88.

U.S. Department of Commerce. <http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf>

Mack, Mary. "Native File Review: Simplifying Electronic Discovery?" *Law Journal Newsletters Legal Tech Newsletter*, Vol. 23, No. 2 (May 2005).

<<http://www.ljnonline.com/alm?It>>.

National Association of Veterans' Research and Education Foundation.

<http://www.navref.org/library/Records_Retention.htm>.

National Council of Nonprofit Associations.

<<http://www.ncna.org>>.

National Institute of Health. Grants Policy Statement.

<http://grants.nih.gov/grants/policy/nihgps_2001/part_ia_7.htm>.

State of Washington, Division of Archives & Records Management, Office of the Secretary of State. "Guidelines for Developing Policy & Establishing Procedures for E-Mail." <<http://www.MERresource.com/libraryRecordsTechnologies/Email>>.

Stephens, David O. and Roderick C. Wallace. *Electronic Records Retention: New Strategies for Data Life Cycle Management*. Lenexa, KS: ARMA International, 2003.

U.S. Department of Health and Human Services. Centers for Medicare and Medicaid Services. <<http://www.cms.hhs.gov/HIPAAGenInfo/>>.