AMVETS Ladies Auxiliary

RECORDS RETENTION

AND

DISPOSITION GUIDELINES

TABLE OF CONTENTS

RECORDS RETENTION AND DISPOSITION GUIDELINES

Introduction

Non-profit organizations need to retain certain records beyond current used needs, according to regulatory, legal, financial and operation requirements.

Whether a record is in paper or electronic format does not determine its value or retention period; its content is the key factor.

How Long to Keep Records

Document Content	Minimum Retention
Accident reports and Claims (settled cases)	7 years
Accounts receivable and payable ledgers and schedules	7 years
Audit reports	Permanently
Bank Statements, deposit records, electronic fund evidence, cancelled checks, reconciliation	7 years
Board Meeting and Board Committee Minutes	Permanently
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

Correspondence, administrative (pertaining to formulation, planning, implementation, interpretation, modification, redefinition of programs, services, projects and the regulations, polices, 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
Correspondence, legal and important matters	Permanently
Correspondence with customers and vendors	2 Years
Deed, mortgages, bills of sale	Permanently
Depreciation schedule	Permanently
Donations	7 years
Employee demographics records	3 years
Employee discrimination reports (EEOC, ADA, etc.)	Permanently
Employment applications	3 years from record creation or personnel action
Expense Analyses and distribution schedules	7 years
Financial Statements, year end	Permanently
Garnishments	7 years
General ledgers, year-end trial balance, journals	Permanently

Form 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
Inventory records	7 years
Journals	Permanently
Loan documents and notes	Permanently
Minute book, including Board and Committee minutes	Permanently
Mission Statement, Strategic plans	Permanently
Notes receivable ledgers and schedules	7 years
Organization charts	Permanently
Payroll records and 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
Property records including costs, depreciation schedules	Permanently
Purchase orders	7 years

Retirement and pension records including Summary Plan Descriptions	Permanently
Sales records	7 years
Tax returns and worksheets	Permanently
Timesheets, books, cards	7 years
Training manuals	Permanently
Vouchers for payments to vendors, employees. etc. (includes employee/office travel and entertainment expense reimbursements)	7 years
Workers compensation documentation	10 year after 1st closure

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. The Records 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 year. The preferred formats are XML for born-digital records, PDF/A for text documents, and TIFF for images.

Migration decisions should be 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. 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 records should be retained

- 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.

- Off-line retention period: data may be stored off-site, typically on magnetic tapes.

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. Originals or copies on CDs and DVDs should be stored in archival CD/DVD cases or Tyvek envelopes 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 in no longer required to be kept, it should be properly destroyed and the destruction should be documented.

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. 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 or financial data.

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

- Hard drives, USB or flash drives, other plug-in type devices: Sanitize by running special software programs or following the manufacture's instructions for full chip erasure. If the drive is no longer operational, cables should be cut and drive disassembled. Its platter 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 default. 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: Degaussing tailored for the type of tape and with proper coercivity. Alternatively, incineration, pulverization, or shedding may be used. If the data sanitizing process is contracted to an outside party, the vendor should sign an agreement state that their practices conform to or exceed the guidelines stated here.