Form 990 Policy Series

The attached Memorandum is a part of the *Form 990 Policy Series*, developed by a group of lawyers, all members of the California bar and practicing nonprofit law (the "Form 990 Policy Series Group"). The *Form 990 Policy Series* includes Memoranda containing rationales and procedures for legal counsel to use in advising their clients on drafting and adopting appropriate policies responding to the new Form 990 as well as form policies and/or questionnaires.

The members of the Form 990 Policy Series Group with respect to the attached Memorandum (posted July, 2011) were as follows: Joel S. Corwin, Co-Chair; Barbara Rosen, Co-Chair; Elizabeth Bluestein; Lani Meanley Collins; the late Gerald A. Laster; Henry Lesser; Nancy McGlamery; Louis Michelson; Joy P. Paeske; Alicia Plerhoples; Lisa A. Runquist; Robert Siemer; Myron Steeves; Patrick Sternal; and Martin J. Trupiano. The views expressed in the Memoranda do not necessarily reflect the views of the law firms or employers at which these lawyers practice or any individual member of the Group.

The date at the top of the attached Memorandum is the date that the Memorandum was finalized, and the Memorandum may not reflect changes in law or practice since that date.

FORM 990 POLICY SERIES
MEMORANDUM

Re: Document Retention and Destruction Policy
Form 990, Part VI, Section B, Line 14 (Form 990 Policy Series Memo #4)

Date: December 1, 2009

NOTE ON THE SCOPE OF THIS MATERIAL

This material is designed to provide general guidance about an aspect of nonprofit corporate governance in the specific and limited context of the governance questions contained in the new IRS Form 990 (published by the IRS in 2008 and applicable to 990 filers based on a 2009-2011 filing year phase-in period depending on the size of the nonprofit). It is intended to provide some general guidance on the establishment of processes and/or policies to address a specific governance question in the Form. The subject matter of that question implicates a broad array of legal and practical issues ranging far beyond the immediate subject matter of the question itself. This material may address some of those issues but does NOT attempt to review them comprehensively and is NOT intended to be relied on for guidance on how they should be addressed in any specific situation.

Whether or not a nonprofit organization adopts a specific governance process or policy (or modifies an existing one), either in response to the disclosure requirements of the new IRS Form 990 or to change its governance practices for other reasons is a matter to be carefully considered by that organization, with input from its board and advisors and evaluation of its specific circumstances. The IRS has explicitly stated that adoption of the policies and practices about which the new Form 990 asks is not mandatory, although the IRS has also indicated that it attaches significance to the manner in which all tax-exempt nonprofit organizations govern themselves. The inclusion of a sample policy in this material is not intended to suggest that the policy is appropriate for every nonprofit organization nor that, if a policy on that topic is determined to be appropriate, the formulation in the sample necessarily fits the needs of an individual nonprofit organization. A customized approach, with outside professional advice, is recommended. Accordingly, this material is intended as general information for legal practitioners advising nonprofit organizations as to their governance and does not constitute legal advice for any particular nonprofit organization.

Although the subject matter of this material may have relevance to nonprofit organizations that are not required to file informational tax returns with the IRS or are permitted to file on an IRS form other than Form 990, the focus of this material is 990 filers. While this material is meant to apply to Form 990 filers who are exempt under Section 501(c) of the Internal Revenue Code, certain portions of this material may be applicable only to Section 501(c)(3) organizations. In addition, although this material may be of assistance with respect to nonprofit organizations that are not subject to oversight under California law, there may be portions of this material that are relevant only to nonprofits organized under, or (by reason of their California-related activities) otherwise subject to, California law and, except as specifically discussed in this material, the laws of other States are not addressed.

---

1. Summary

The new Form 990, at Part VI, Section B, Line 14, asks whether the organization has a written document retention and destruction policy. As stated in the new Form 990 Instructions: "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." This Memorandum is intended to provide general guidance for the consideration and adoption of a policy responsive to the Form and Instructions.

2. Rationale for Adoption of the 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. Paper storage took up a lot of space, either at the organization premises or at off-site storage facilities which charged for the service. Even with the dawn of the electronic records era, storage space and the cost of that space continued as an issue. Initially, records would be stored on magnetic cards or disks, which themselves also took up space, although not as much physical space as paper documents. At the same time, the electronic storage media themselves could become costly for an organization. Later, electronic records, including e-mails, were stored on servers maintained by the organization at its premises and/or off-site. As clients have indicated, this method of storage has also become costly, with the requirements of maintaining servers capable of storing vast amounts of data.

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.

3. Background of Requirements/Sources for the Policy

A. Specific Retention Period Requirements for Different Documents

State and federal laws with respect to statutes of limitation for particular lawsuits as well as specific requirements for retaining certain documents will largely determine the retention period for affected documents. At the same time, certain documents are of such importance to an organization that they should be permanently retained.

B. Sarbanes-Oxley Requirements

Section 802 (Criminal Penalties for Altering Documents) of the Sarbanes-Oxley Act ("SOX") 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."

C. 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.

D. Zubulake and Other Cases

In a series of five opinions involving an employment discrimination case (Zubulake I-V), the U.S. District Court for the Southern District of New York dealt with a number of issues relating to electronic discovery. In *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("Zubulake I"), the court dealt with the scope of electronic discovery and the issue of who should pay for it. **As indicated in Zubulake IV, 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.

The holdings of these cases, as well as others like them, are relevant to the drafting and implementation of a DRD Policy. In that regard, taking into account such cases as well as the Federal Rules as they relate to electronic discovery, the DRD Policy should also 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.

E. Form 990 and Instructions

Part VI, Section B, Line 14 of the new Form 990 asks: "Does the organization have a written document retention and destruction policy?" The new Form 990 Instructions relating to this topic state:

> 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. Answer "Yes" if the organization had these policies in place as of the last day of the organization's tax year.

Certain federal or state laws may … prohibit destruction of certain documents. For instance, while the federal Sarbanes-Oxley legislation generally does not pertain to tax-exempt organizations, it does impose criminal liability on tax-exempt as well as other organizations for … destruction of records with the intent to obstruct a federal investigation. See 18 U.S.C. section… 1519. Also note that an organization is required to keep books and records relevant to its tax exemption and its filings with the IRS. …

4. <u>Considerations and Procedures for Implementation of the Policy</u>

A. First, discuss with the client 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, the client 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 or customers. 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 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.

Thus, the policies should be structured in such a way that the only (or primary) responsibility of volunteers with respect to documents would be to produce specifically identified documents upon request of management, if the volunteer still retained such documents. For example, the policy might provide that, after each project in which a volunteer has been involved, or each term which the volunteer has served, it would be the responsibility of the policy administrator to confirm whatever types of documents the volunteer retained and to request any such documents which such administrator felt would be necessary for retention by the organization (not by the volunteer). Other outsiders may include, without limitation, lawyers, accountants, bookkeepers, human resources providers, vendors and other service providers. Lawyers have their own special responsibilities with respect to documents. Depending upon the sensitivity of the documents involved with the particular vendor relationship, the organization's contract with the vendor could specify particular responsibilities of the vendor with respect to documentation. However, make no mistake about it, the primary responsibility with respect to document retention and destruction for an organization rests with management.

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. However, by all means, only include requirements which management knows will be met within the capabilities of the organization. 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 CEO, then the administrator should report to the CEO.

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. Again, it cannot be stressed enough, that the organization should only adopt policies which it is confident it can follow.

J. 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.

In every case, the policy must be disseminated to all affected constituencies such as, for example, employees, directors, members and volunteers. Finally, the client should be cautioned that 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.

5. Sample Policy or Policies

****

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 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 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 counsel's own research and determination as to appropriate periods.]

Document Type	**Retention Period**
Accounting and Finance	
Accounts Payable	7 years
Accounts Receivable	7 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.

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

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

****