Records Management and Retention Policy

California Nonprofit Public Benefit Corporation

Made possible through the support of the **Annenberg Foundation**

About This Form: Public Counsel's Community Development Project has designed the attached form of Records Management and Retention Policy for a California Nonprofit Public Benefit Corporation to assist nonprofit organizations seeking to adopt or amend such a policy and the pro bono attorneys who represent them.

This form is annotated with explanatory endnotes, including citations to applicable laws, alternatives and recommended practices. For further instructions on how to use this form, how to create a policy that will allow a corporation to answer "yes" to Part VI, Question 14 on the IRS Form 990, and how to implement this policy, please see the endnotes. Public Counsel will update this form periodically for changes in law, recommended practices and available resources.

Important Notes: In creating any corporate policy, it is very important that a nonprofit corporation institute procedures that the corporation is likely to be able to comply with consistently in the long term. Therefore, this sample should be used only after carefully considering every provision. A corporation should not adopt any provisions that will be too burdensome for the corporation to follow given its circumstances. A policy will not protect a corporation from liability if it is not followed, and in some cases, a failure to consistently follow a written policy may lead to more liability for the corporation than if no written policy existed. Please see the first endnote for more information.

***This form should not be construed as legal advice*.** Please contact an attorney for legal advice about your organization's specific situation. This sample should not be used "as is" but should be modified after careful consideration of the explanations in the endnotes. Some corporations may need to include additional provisions not discussed in this form to comply with laws applicable to specific types of organizations.

...

Public Counsel's Community Development Project provides free legal assistance to qualifying nonprofit organizations that share our mission of serving low-income communities and addressing issues of poverty within Los Angeles County. If your organization needs legal assistance, or to provide comments on this form, visit *www.publiccounsel.org/practice_areas/community_development* or call (213) 385-2977, extension 200.

FORM OF RECORDS MANAGEMENT AND RETENTION POLICY FOR A CALIFORNIA NONPROFIT PUBLIC BENEFIT CORPORATION

* * *

RECORDS MANAGEMENT AND RETENTION POLICY[1]

OF

[NAME OF CORPORATION]

A California Nonprofit Public Benefit Corporation

ARTICLE I INTRODUCTION

Section 1. **[Name of Corporation]** ("Corporation") requires its directors, officers, employees, volunteers, agents, and other personnel (all such persons are referred to in this Policy as "Corporation personnel") to observe high standards of business and personal ethics in the conduct of their duties and responsibilities. The purpose of this Records Management and Retention Policy ("Policy") is to ensure that all Records (as defined in Section 3 of this Article) necessary for business and compliance reasons will be retained for a period of time that will reasonably assure their availability when needed, but for no period of time longer than reasonably necessary for the purposes for which the data was collected. This Policy is intended to support Corporation's endeavors to comply with state, federal, and international laws[2] governing the destruction of documents and records applicable to nonprofit and charitable organizations.

Section 2. It is the policy of Corporation to retain and manage all Records in accordance with uniform guidelines, practices, and procedures. All Corporation personnel shall manage, protect, and maintain all Records in accordance with the Records retention schedule ("Retention Schedule," attached as Schedule 1) and this Policy.[3]

Section 3. "Records" means all documents, files, or records created by any Corporation personnel while acting within the course and scope of his or her duties pertaining to Corporation business or operations, or copies of any of the foregoing, in any format or medium, including but not limited to: computer records, electronic mail ("e-mail"), voice mail messages, text messages, instant messages, handwritings, photographs, photocopies, or facsimiles, regardless of the manner in which the record has been stored. Specific categories and types of Records are contained in the Retention Schedule.

Section 4. All Records required to be retained to document Corporation's legal compliance, or otherwise required by law, rule or regulation to be retained, shall be retained for the periods required by law as described in the Retention Schedule. All Records required to be retained due to pending or threatened litigation or investigation shall be retained for so long as the litigation or investigation is active, plus any additional tail period as may be provided for in this Policy and the Retention Schedule.

ARTICLE II SCOPE

Section 1. All Records pertaining to Corporation business maintained or created by any Corporation personnel,[4] including any Records retained off Corporation property, are subject to the requirements of this Policy.[5] The format of Records to be retained may vary, e.g., hard copy original, photocopy, facsimile, microfilm, microfiche, computer file, e-mail, computerized image. Regardless of the format selected, Records must be safeguarded and easily accessible.

In addition to paper Records, this Policy applies to all electronic Records, whether or not stored on Corporation-issued devices, including Records created or maintained by Corporation personnel remotely, such as on home personal computers, laptops, tablets, phones, other devices, back-up drives, or the internet on cloud platforms (e.g., Google Drive, Apple iCloud, Netflix, Yahoo Mail, Dropbox and Microsoft OneDrive).[6, 7]

Section 2. To the extent possible, the Record retention guidelines contained in this Policy should apply to all applicable Records created, maintained, stored, or otherwise in the possession of Corporation's third-party vendors.[8]

ARTICLE III LEGAL HOLD[9]

Section 1. Retention procedures will be suspended when a Record or group of Records are placed on legal hold ("Legal Hold"). A Legal Hold requires preservation of appropriate Records under special circumstances, such as litigation, government investigations, or consent decrees. In the event that Corporation's Board of Directors or management learns of any claim that could reasonably give rise to litigation or government investigation, Corporation shall consult with legal counsel as to the need for a Legal Hold.[10] In such case, Corporation, in consultation with legal counsel, will determine and identify what Records are required to be placed under a Legal Hold.

Section 2. Corporation will notify individual Corporation personnel if a Legal Hold is placed on Records for which the individual is responsible.[11] The individual is then required to locate, index, and protect the necessary Records. Any Record that is relevant to a Legal Hold must be retained and preserved. If the individual is unsure whether a Record is relevant to a Legal Hold, the individual should protect that Record until he or she receives clarification from his or her supervisor following Corporation's consultation with its legal counsel.[12] FAILURE TO COMPLY WITH A LEGAL HOLD MAY RESULT IN SIGNIFICANT RISK, EXPOSURE, OR LIABILITY TO CORPORATION.

Section 3. A Legal Hold remains effective until it is released in writing by Corporation after consultation with legal counsel. Following the final resolution of the relevant litigation, government investigation, or consent decree, Corporation will consult with legal counsel as to the release of the Legal Hold. After the individual receives written notice from Corporation, the individual may return all Records relevant to the Legal Hold to his or her normal retention procedures.

ARTICLE IV ADMINISTRATION

Section 1. This Policy is to be administered by the ***[insert appropriate individual, department, or division]***. Questions regarding this Policy should be directed to the **[insert title]** of the applicable department, division, or business unit, or to **[insert title of individual responsible for overall administration of the Policy]**[13]

Section 2. Guidelines for retention of Records are provided for in the Retention Schedule. Any changes to the Retention Schedule must be approved by the [**Records Management Committee**[14]]. ***[Insert optional language delegating to each corporate department the obligation to identify needed changes to the Retention Schedule]***.[15]

Section 3. All Records shall be created, maintained, and stored in a manner that complies with Corporation's Records storage, accessibility, and retrieval procedures as well as Corporation's privacy and data security policies and procedures.[16]

Section 4. Records kept on-site should be destroyed in accordance with the Retention Schedule.[17] Records that are sent off-site shall be labeled with a destruction date.

Each ***[month]***,[18] the [**insert title of individual responsible for overall administration of the Policy**] will review a list of all Records that have reached the destruction date, will confirm that the Records can be destroyed, and will decide whether any such Records are the subject of a Legal Hold to ensure Corporation's continued ability to produce Records for known investigations or litigation.[19] [Corporation shall maintain a schedule of Records that have been approved for destruction and the dates that any Records are destroyed.]

If Corporation uses an outside vendor for storage and/or destruction of Records, after approval for destruction, the Records storage vendor shall shred or otherwise destroy the noted Records in the manner specified by Corporation and provide a certificate of destruction in accordance with this Policy. Confidential Records shall be destroyed only by secure means.

Destruction of electronic Records shall utilize a method to ensure the electronic Records are completely and securely destroyed and not retrievable from any storage media.

Section 5. The **[Records Management Committee]** shall meet **[periodically]**[20] to review and, if necessary, update this Policy to comport with changed business practices and systems and new or amended laws or regulations. Any changes to this Policy must be approved in writing by Corporation's ***[Board of Directors OR Records Management Committee OR Executive Director]***. Changes will be distributed to relevant Corporation personnel.

Section 6. Failure to comply with this Policy may result in disciplinary action, up to and including termination of employment, volunteer, or board member status.

* * *

Adopted by the Board of Directors at its Meeting on _____.

[1] **HOW TO USE THIS FORM:** This sample records management and retention policy has been developed for use by small and mid-sized California nonprofits for educational purposes only. The endnotes discuss the applicable law, recommended practices, and why certain language has been included. **Bold** and ***bold italicized*** bracketed language in this form indicates that information specific to the corporation adopting this policy must be inserted. Italicized bracketed language in this form indicates optional language. In such cases, the endnotes will explain under what circumstances a corporation would include or delete this language.

***Important Note*: In creating any records retention policy, it is very important that a nonprofit corporation institute only procedures that the corporation is likely to be able to comply with consistently in the long term. A records retention policy will not protect the corporation from liability as described below if it is not followed, and in some cases, a failure to consistently follow a written policy may lead to more liability for the corporation than if no written policy existed.** Each user of this form should think through every provision carefully and should not include any provisions that will be too burdensome for the corporation to follow under its circumstances. For this reason, this form policy contains a simple outline of basic procedures, with additional suggested language in the endnote annotations that may be considered by larger corporations with more resources for compliance. **If adopting a records retention policy, a corporation should, at a minimum, include the requirement that various records needed for various legal reasons should be retained for the required time periods, as indicated in Schedule 1, and that ALL RECORDS DESTRUCTION SHOULD CEASE IMMEDIATELY, AND THE CORPORATION SHOULD CONSULT LEGAL COUNSEL, WHEN THE CORPORATION LEARNS OF A CLAIM THAT MAY GIVE RISE TO A GOVERNMENT INVESTIGATION, LITIGATION, OR ANOTHER OFFICIAL PROCEEDING.**

Why adopt a Records Management and Retention Policy? A corporation is not required by law to have a records management and retention policy. However, the Internal Revenue Service ("IRS") asks nonprofit tax-exempt organizations to report in their annual Form 990 filings as to whether they have such a policy (IRS Form 990, Part VI, Question 14, available at *https://www.irs.gov/pub/irs-pdf/f990.pdf*). As stated in the instructions to Form 990, in order to answer "yes" to this question, an organization must, at a minimum, have a policy in place as of the last day of the organization's tax year that 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 (IRS Form 990 instructions, available at *https://www.irs.gov/pub/irs-pdf/i990.pdf*). While this policy is not required by law, the IRS suggests that such a policy promotes good tax compliance.

More fundamentally, however, a records retention policy helps a corporation comply with applicable laws and regulations and protect itself from liability. Various aspects of a corporation's operations are subject to substantive laws and regulations that include recordkeeping obligations. Failure to provide these records on audit may give rise to penalties. Records are often the best way of proving to law enforcement and regulatory agencies that a corporation has complied with laws and regulations. For example, in a tax audit, the corporation will have the burden to prove that the information reported on its tax returns is correct. Without accurate and reliable records, the corporation may not be able to meet this burden. A records retention policy will prevent the inadvertent destruction of records needed for legal or business reasons.

A records retention policy can also save costs, because appropriately stored and retrievable records will permit cost efficient records recovery when needed, and establishing a schedule for regularly disposing of unneeded records will avoid unnecessary storage costs.

Finally, a sound records management and retention policy can be an important aid in responding to claims or litigation against the corporation, in order to prove the corporation's defense and to avoid criminal penalties for destruction of evidence or monetary sanctions for failure to provide records that are requested in connection with litigation. Consistent compliance with a records management, retention, and destruction policy will help a corporation show that it has not illegally destroyed evidence with the intent of obstructing an investigation or litigation, because the corporation will more readily be able to find and produce applicable records, and because the corporation will more readily be able to show that any destruction was done not for the purpose of obstruction, but for the purpose of systematically removing obsolete records to save on storage costs.

[2] The European General Data Protection Regulation ("GDPR") became effective May 25, 2018 and applies to organizations located within the EU but also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing (e.g., collection, use, storage, disclosure, etc.) and holding the personal data of data subjects residing in the European Union, regardless of the company's location. Violations of the GDPR can result in fines up to 20 million euros, or up to 4 % of global turnover of the preceding fiscal year, whichever is higher. GDPR Article 83. A records retention policy that includes processing of European personal data must be critically analyzed if applicable to an organizations' practice. Consult with an attorney to determine whether your organization's activity and practices will trigger GDPR requirements.

[3] This form of records retention policy comprises (1) the policy itself, which states that the corporation will maintain a consistent method of creating, storing, and destroying records and provides procedures for administration of the policy, (2) appendixes that provide examples a corporation may wish to use for notification forms, a sample electronic communications policy, and a form to use when removing records from storage, and (3) a list contained in **Schedule 1** as to what amount of time an organization should retain records in each of various categories, to provide guidance for staff and volunteers as to how many years to retain various types of records that may be needed for future legal or business reasons. It is also acceptable to create a records retention policy that incorporates a list similar to **Schedule 1** within the text of the policy itself. Any such list should not be used "as-is" but should be modified to reflect the types of records that the corporation uses in its operations or that are relevant to its exempt purpose. See the annotations to **Schedule 1** for more commentary on this topic.

[4] Users of this form should recall that the term "personnel" includes volunteers. The form includes volunteers in order to comply with the description of a document retention policy provided in the instructions to the IRS Form 990. Thus, any of the corporation's records that are created by volunteers are also subject to this policy, and it is important to ensure that all volunteers are made aware of this policy. Corporations that have volunteers who work from home and create important records for the corporation, especially if those records are housed on a volunteer's computer rather than a computer owned by the corporation, should consider including an additional statement here that the final version of any records created by volunteers should be transferred to one of the corporation's computers for storage in a manner consistent with other corporation records. If the nature of the corporation's operations makes it necessary for corporation volunteers to retain records in their own computers or homes, the corporation should implement and consistently monitor procedures that will safeguard important corporation records for future retrieval. Additionally, for purposes of the GDPR, all expectations and obligations of personnel should also include any individual that has contact with data subjects' data, regardless of a record of it.

[5] For a corporation that has multiple departments or divisions with separate department or division managers, it is not necessary for each department that handles a record to be responsible for maintaining a copy of that record. A corporation in this situation should determine which department or division has the responsibility for maintaining the various categories of records in accordance with the policy. Such large corporations may want to include a provision to that effect within the policy, such as the following:

"*The Record retention guidelines contained in this Policy apply only to the originating department responsible for action related to the Record(s) and, where indicated, to other departments receiving copies of these Records. Where multiple departments are responsible for action related to a single Record, those departments should agree as to which will be responsible for Record retention and document such responsibility. The objective is to minimize the number of copies kept while ensuring that documents are retained as required.*"

[6] As part of any retention policy and related documents, Corporations may also want to include GDPR deletion requirements. Under the GDPR, the right to erasure – or the Right to Be Forgotten under Article 17 – gives data subjects the right, with exceptions, to require a company to immediately erase personal data when it is no longer needed for the original processing purpose, the data subject has withdrawn consent and there is no other legal ground for processing, the data subject has objected and there are no overriding legitimate grounds for processing, or erasure is required to fulfill a statutory obligation under the EU law or the right of the Member States.

[7] If the Corporation is to be GDPR-compliant, contact an attorney to determine whether the following language applies to your organization and should be included:

"*In order to adhere to international privacy laws and standards, this Policy also applies to the processing of all personal data by Corporation.*"

[8] Corporations that use outside vendors who will create and maintain records subject to this policy may want to consider requesting or requiring that these vendors comply with the policy. A corporation that has the capacity or leverage to require its vendors to comply with the records management and retention policy may consider adding to the policy the following language:

"*Applicable vendor agreements should include language that requires the outside vendor to comply with the terms of this Policy.*"

In the alternative, a corporation that has the capacity to monitor all records created by outside vendors, and maintain and store all of such records, may require instead that any vendors with control over corporation records must provide the original records to the corporation promptly so that the corporation can maintain the records consistently with the policy.

[9] Federal law prohibits all corporations, including nonprofit corporations, from destroying, altering, concealing, falsifying or otherwise covering up documents and records, or attempting to do so, with the intention of impeding, obstructing or influencing government investigations or official proceedings. This is part of the law commonly known as "Sarbanes-Oxley." *[18 U.S.C. § 1519]* Violation of these rules is a crime and can result in penalties or imprisonment. In addition, destruction or spoliation of evidence, including records and documents, that are relevant to pending litigation can give rise to civil liability and penalties. This is one important reason why corporations adopt records retention policies that include a fixed schedule for destroying unneeded records. If a corporation establishes and consistently follows a set schedule to destroy records that are no longer needed, the corporation can avoid incurring unnecessary storage costs. However, if a corporation instead destroys records haphazardly, only at times when storage is full and without a set procedure in place, there may be a risk that the corporation will inadvertently destroy records close in time to a pending litigation or investigation, which may give rise to the perception that it is acting with illegal intent.

In order to ensure that a corporation complies with laws relating to records destruction, **any records retention policy that permits the destruction of records after a period of time must contain a procedure for stopping or placing a "hold" on destruction of records related to pending investigations or litigation.** A corporation is not required to continue to store every unrelated record just because litigation has been filed but is required to retain all records it knows or reasonably should know would be relevant to the case. *[See, e.g., William T. Thompson Co. v. Gen. Nutrition Corp., 593 F. Supp. 1443 (C.D. Cal. 1984)]* Therefore, in the case of a legal hold, the corporation must have a means of determining which records are relevant and hold the relevant records until the litigation or investigation concludes. This Article is one example of such a legal hold provision that indicates when a corporation should consult with legal counsel about establishing a legal hold and provides that legal counsel will determine at that time what records are subject to the hold. If a user of this form wishes instead to write in procedures for how to determine which records are relevant to any particular case or investigation, experienced legal counsel should be consulted when drafting the policy. It may not be possible in all instances to determine in advance which categories of records must be retained upon learning of a claim or investigation. Therefore, **it is strongly recommended that any corporation consult legal counsel upon learning of any claim that is likely to give rise to litigation, investigation, or other official proceeding.**

[10] It is always good practice for a corporation to consult with legal counsel as promptly as possible when learning of a claim that is reasonably likely to give rise to a government investigation, litigation, or other official proceeding. In any such consultation, a corporation that has adopted a records retention and destruction policy should cease destruction of records until it has consulted with counsel and should request that counsel advise on the need for, and records categories subject to, the legal hold. Smaller nonprofits that do not have a general counsel or other attorney that advises the corporation on a day-to-day basis should be sure to consult an attorney in these circumstances. A nonprofit that has a general counsel should ensure that the general counsel is involved in the drafting and administration of this policy and all legal holds.

[11] To ensure that the same information is given to personnel every time a legal hold is placed on any corporation records, the corporation may consider adopting a standard form of notification to be sent either to all personnel

or to relevant records retention personnel every time a legal hold is imposed. An example of such form is attached to this policy as **APPENDIX A**. If adopting such a form, this policy should state that immediately upon the commencement of every legal hold, a notification in this form will be given to personnel, and the corporation should also adopt a form that will notify the same personnel of the termination of the legal hold (an example of such termination form is attached to this policy as **APPENDIX B**). If adopting such forms, the corporation must make sure to use them in the case of every legal hold and should provide a copy of the forms to any legal counsel who is advising on the litigation or investigation (and/or the legal hold) to determine what information must be included. If the user of this form policy chooses to adopt such procedures, an additional paragraph may be added to this section of the policy stating:

*"See **APPENDIX A** for a sample Legal Hold Memorandum and **APPENDIX B** for a sample Legal Hold Release. Corporation's legal counsel will tailor the Legal Hold Memorandum and Legal Hold Release to fit the facts of a particular litigation or investigation matter."*

[12] Alternatively, a corporation can designate one person to handle all inquiries regarding a legal hold. In such case, this sentence should be replaced with language such as the following:

*"If the individual is unsure whether a Record is relevant to a Legal Hold, the individual should protect that Record until he or she has consulted with **[insert title of individual responsible for overall administration of the Policy]**."*

[13] Each corporation should take active measures to train its directors, officers, employees, volunteers, agents, and other personnel to make sure that the Policy's procedures are implemented properly and tracked effectively.

If Corporation is required to be GDPR-compliant, contact an attorney to determine whether the following language applies to your organization and should be included:

"*Corporation has appointed a Global Privacy Officer ("GPO") [or equivalent; if necessary] with expertise in applicable privacy and data protection laws to oversee the development, implementation, and enforcement of this Policy. Corporation seeks to ensure timely and appropriate involvement of the GPO, or his or her designee, in all issues involving Corporation's processing of personal data. The GPO has direct access to Corporation's leadership."*

[14] Corporations with staffs so large that the executive director/CEO cannot reasonably be expected to monitor day-to-day compliance with the policy should consider establishing a Records Management Committee of a few select employees from business, legal, and information technology. Such a committee would have the responsibility to monitor and evaluate the policy and make recommendations to the board of directors for adoption of any necessary policy amendments. If there is not a Records Management Committee, it would generally be a board responsibility to evaluate the policy for revisions. If no committee is established, all references in this policy to a Records Management Committee might be replaced with the title of the executive director or such other officer as can monitor these issues for the corporation.

[15] For corporations with fairly large departments or divisions, where it would be more efficient to identify any necessary changes to the retention schedule at the department or division level rather than at the broader corporate level, users of this form should consider whether to include an additional provision at the end of this section that delegates to each department or division the obligation to establish its own procedures for identifying needed modifications to the retention schedule, which would then be communicated to the administrator of the policy (whether that administrator be a committee or a single management official). Such a provision could read as follows:

"*Consistent with this Policy, each Corporation department or division shall establish procedures to identify and communicate to the **[Records Management Committee]** for approval, any necessary modifications or additions to the Retention Schedule:*

(a) By category of Records which are to be retained;
(b) By the manner in which Records are to be safeguarded;

(c) By the retention period for each type of Record; and
(d) By the indexing and retrieval system to be used."

[16] If the corporation does not have already-established file creation, management, and storage procedures, users of this form may consider including in this section a description of these procedures. However, such procedures need not be contained within the text of the policy, and can be established separately, either on an individual department or division basis or for the corporation as a whole.

Record creation and indexing procedures: Standardizing procedures for records creation, indexing, and management can make retrieval of these records for purposes of legal compliance, business use, and ultimate destruction much easier and more cost-effective. In addition to saving time and expense, a uniform method of creating and indexing records that is consistently followed will help corporation management to feel comfortable certifying, in any litigation, investigation or audit context, that it is providing to the relevant authorities all existing records in a requested category. A corporation should not establish policies or procedures that its personnel cannot consistently follow (for example, due to lack of resources or staffing), because a failure to follow established procedures could increase risks of liability by, for example, giving rise to an inference that the corporation is not providing all relevant records or is otherwise impeding an investigation. When establishing such procedures, users of this form should consider the following issues and address them in a way that increases the likelihood of consistent application:

- What conventions or standards are used in naming, numbering, indexing, and filing file folders?
- What requirements or guidelines are used for the location and structure of paper file folders, cabinets, filing, storage, etc.?
- What type of electronic record management system is used?
- Does the electronic record management system permit the capture of metadata relating to the electronic record, including author, name of record, description of record, department, type or category of record, date created, dates modified, retention period, etc.?
- What conventions or standards are used in naming, describing, and categorizing electronic files and file folders?

Record storage procedures: In establishing record storage procedures, users should consider the following issues:

- Confidentiality and security of records that are required to be so maintained. Examples of information that might be required to be safeguarded include patient information in the hands of a healthcare provider, privileged information in the hands of a legal services provider, credit information or other identifying information about donors or clients that pay for services, contact information collected for commercial purposes and subject to a website privacy policy, etc.
- Reasonable accessibility of stored records. Active records in storage should be readily accessible by the corporation. Inactive records do not need to be readily accessible but must be stored in a system and in a format that permit identification and retrieval if necessary.
- Preservation of records from damage. For example, a corporation may wish to avoid storing records near plumbing lines and should safeguard records from other hazards.

Electronic Records: Users of this form should also keep in mind that emails and other records kept in electronic format are not exempt from record retention laws. *[See, e.g., Fed. R Civ. P. 26 and Cal. Civ. Proc. § 2031.010]* These records provide separate challenges for storage, however, because they are subject to issues such as computer failure and are also easier to alter at a later date. A corporation is not required to print and store in paper form all such records but must make good faith efforts to protect their integrity. If a corporation makes such efforts and follows a consistent policy with regard to retention, the corporation may avoid monetary

sanctions for accidental loss of electronic records. *[See, e.g., Fed. R Civ. P. 37, providing that, absent exceptional circumstances, sanctions will not be imposed for failing to produce electronically stored information that has been lost in the routine, good faith operation of an electronic information system; and Cal. Civ. Proc. § 2031.060, providing that, absent exceptional circumstances sanctions will not be imposed for failing to produce electronically stored information that has been lost, damaged, altered, or overwritten as the result of the routine, good faith operation of an electronic information system.]* One example of a reasonable preservation effort would be maintaining anti-virus software on computers used to store records.

It is good practice for a corporation whose personnel use e-mail in carrying out their employment duties to institute an *Electronic Communication Policy* either as a component of an employee handbook or separately. The purpose of such a policy is to make employees, contractors, volunteers, and other users aware of what the corporation deems as acceptable and unacceptable use of its e-mail system. When drafting record creation, indexing and storage policies, it is important to make sure that the procedures outlined in those policies are consistent with any *Electronic Communications Policy* that the corporation may have previously adopted. An example of such a policy can be found in **APPENDIX C.**

Discovery Rules: Users of this form should also consider state and federal discovery rules when establishing electronic record storage systems and procedures to ensure compliance in the event of litigation. The California Electronic Discovery Act (the "Act") largely mirrors the Federal Rules of Civil Procedure governing electronic discovery and provides that parties may demand copying, testing, sampling, or inspection of electronically stored information. Both the Federal Rules and the Act permit the requesting party to specify the form in which the information is to be produced. If no form is specified, the responding party may produce the information in the form in which it is ordinarily maintained or in a form that is reasonably usable. [*See, Fed. R Civ. P. 34; Cal. Civ. Proc. § 2031.030]*

Similarly, a party is generally not required to produce electronically stored information that is from a source that is not reasonably accessible because of undue burden or expense. Unlike the Federal Rules, however, the Act places the burden on the responding party to bring a motion for a protective order or to make written objections to such a request. *[See, Cal. Civ. Proc. § 2031.060]* The Federal Rules, in contrast, place the burden on the requesting party to move to compel if the responding party claims that the information is not reasonably accessible. *[See, Fed. R Civ. P. 26(b)]*

[17] It is extremely important that a corporation adopting a records retention policy comply consistently with the records destruction schedule with regard to all records.

[18] Depending on the volume of records prepared by a corporation in any given month or other period, the corporation should consider whether to review the records for destruction each month or at some longer time-period that is feasible and will not create an undue burden on corporation personnel.

[19] In a large corporation with various departments that may have needs for the same records, and no single officer or employee who would be aware of all such needs, the corporation should consider adding a provision that each such department should be consulted before records are destroyed. In such case, this paragraph should be replaced with language such as the following:

*The **[insert title]** of each department, division, or business unit will receive each [month] a report of all records ready for destruction. Each department, division, or business unit will be asked to confirm that the records can be destroyed and then the destruction will be approved by Corporation's **[insert title]** to ensure Corporation's continued ability to produce records for known investigations or litigation.*

[20] The frequency of policy review is discretionary and should be tailored to the needs of the corporation. A large nonprofit with many records storage needs may prefer to require at least annual review meetings, whereas a start-up nonprofit that does not generate a large number of records, or that has been in existence for a short time and has not yet reached the destruction date for most of its records, may want to be more flexible as to when a review of the policy would be required.

FORM OF RECORDS MANAGEMENT AND RETENTION POLICY FOR A CALIFORNIA NONPROFIT PUBLIC BENEFIT CORPORATION

* * *

RECORDS MANAGEMENT AND RETENTION POLICY

SCHEDULE 1: RETENTION SCHEDULE

ARTICLE I. INTRODUCTION

In accordance with Corporation's Records Management and Retention Policy ("Policy"), this Schedule 1 ("Retention Schedule") sets forth retention periods applicable to Records held by Corporation, wherever stored. To the extent that a Record is included in more than one category, the longer retention period shall apply. Records which are (i) not identified in the Retention Schedule, (ii) no longer needed for Corporation business or operations and (iii) not subject to a Legal Hold, should be promptly destroyed.[1]

ARTICLE II. DEFINITIONS

Section 1. **Active / Inactive Records**. Records may be classified as either "Active" or "Inactive" Records.

(a) "Active Records" are Records that are regularly referenced or required for current uses. A Record is considered Active if it meets at least one of the following criteria:

(1) There is a regulatory or statutory requirement to keep a Record;

(2) It would be advantageous to Corporation to be able to access a Record quickly;

(3) A Record will be needed for reference at a specific time in the future; or

(4) The custodian of the Record makes the determination that a Record may be retained as an Active Record.

(b) "Inactive Records" are those Records that are no longer needed for current business. Inactive Records are those Records that need not be readily available but still must be retained for legal, fiscal, operational or historical purposes. Inactive Records may be archived at a remote location(s).

Section 2. **"C + x":** Refers to a retention period, in which "C" refers to the year of the Record's creation or acquisition, and "x" refers to the number of additional years the Record is to be kept

after its creation or receipt. For example, a retention period indicated as *C + 3 years* means that a Record is to be kept for three years after the year of creation or acquisition.

Section 3. **"A + x":** Refers to a retention period, in which "A" refers to the year the Record's Active period expires (or when the Record becomes Inactive), and "x" refers to the number of additional years the Record is to be kept after the expiration of its Active period. For example, a retention period indicated as *A + 3* years means that a Record is to be kept for three years after the year the Active period expires (i.e., three years after the Record becomes Inactive).

ARTICLE III. EXCEPTIONS

Section 1. **Legal Hold.** All Records required to be retained due to pending or threatened litigation or investigation shall be retained for so long as the litigation or investigation is active. (See Article III of the Policy, "Legal Hold").

Section 2. **Contractual Requirements.** To the extent that contractual records retention requirements exceed the retention periods in this Retention Schedule or specify the retention of Records not listed in the Retention Schedule, the contractual requirements will control. No originals of Records related to open contracts and subject to contractual retention requirements may be destroyed without the approval of Corporation's **[insert title of the individual responsible for overall administration of the Policy]**, who will consult with other Corporation management personnel, as necessary.

ARTICLE IV. RETENTION SCHEDULE

Important note: *This template Retention Schedule shows various categories of documents that may be applicable to Corporation. The Retention Schedule* ***should not be used as-is****, but must be modified to (a) meet legal, regulatory and business retention requirements of Corporation, and (b) reflect specific records categories and descriptions applicable to Corporation.*[2]

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
PROGRAM OPERATIONS			
Purchasing / Procurement Contracts	**Contracts evidencing or relating to Corporation's purchasing of goods and services, and fulfillment of customer orders**	A + 10 years	Business Reasons[3]; Statute of Limitations
Purchasing / Procurement Records Other than Contracts	**Records other than contracts evidencing Corporation's purchasing of goods and services** (e.g., vendor invoices, delivery receipts, receiving documents)	C + 10 years	Business Reasons; Statute of Limitations
Inventory Management	**Records relating to inventory** (e.g., inventory counts, back orders, returns, pick investigation forms, freight outbound and inbound)	C + 6 years	26 CFR 301.6501(e)-1 (IRS); 26 U.S.C. 6501(e) (6 years); Statute of Limitations

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
Shipping (non-contracts)	**Records (not including contracts) relating to shipping services used by Corporation** (e.g., invoices, shipping records, regarding Standard, Roadway, Yellow Freight, Fed Ex, UPS)	C + 3 years	Business Reasons
ACCOUNTING AND FINANCE			
Bank Records	**Records relating to Corporation's ordinary banking activities** (e.g., bank statements, bank reconciliations, bank deposits, cancelled checks, check listings / ledgers / registers, petty cash, wire transfers, electronic payment records)	C + 10 years	26 CFR 301.6501(e)-1 (IRS) (6 years); Statute of Limitations
Financial Statements	**Periodic Financial Statements** (e.g., periodic audited and un-audited financial statements, including balance sheets, income statements and profit and loss statements, audit work papers)	Annual – Permanent Others – C + [10] years	Business Reasons; Statute of Limitations
Financial Planning	**Records relating to financial planning and budgeting** (e.g., financial forecasts, pro forma financial statements, budgets, business plans)	A + 3 years	Business Reasons
Accounting	**Records relating to Corporation's current accounting functions** (e.g., accounts payable invoices~~;~~, accounts payable and receivable ledgers~~;~~ general ledgers~~;~~ charge offs~~;~~ uncollectible accounts~~;~~ travel, entertainment and expense reports, chart of accounts, trial balance, cost accounting, journals)	A + 10 years	26 CFR 301.6501 (IRS) (6 years)
Taxes	**Records relating to income and other taxes paid by Corporation** (e.g., work papers, returns, schedules, IRS forms, correspondence, IRS audit reports, internal audit work papers, depreciation schedules)	A + 7 years (A = the later of when return filed or return due date)	26 CFR 301.6501 (IRS) (6 years); 18 Cal. Code Reg. § 4901(i) (4 years)
Loans / Financing	**Records relating to Corporation loans** (e.g., bank loan documents and records, bond documents)	A + 10 years (A = Until loan paid in full)	Business Reasons; Statute of Limitations
CORPORATE RECORDS / GENERAL OPERATIONS			
Organizational / Corporate Governance Documents	**Records relating to the formation, organization, governance and tax-exempt status of Corporation** (e.g.,	Permanent	Business Reasons; Statute of Limitations; Cal. Corp. Code §§ 6320

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
	Articles of Incorporation, Bylaws, Minutes of Board meetings, Minutes and reports of Board Committee meetings, Minutes of Member meetings, Organizational charts of affiliates and management personnel, Annual Member Reports, Resolutions / Records of Action taken by Members without Meeting, IRS determination letter recognizing tax-exempt status, application for recognition of tax-exempt status)		
General Corporate Operations	**Records relating to general operations of Corporation.** (e.g., Qualification to do business, Corporate spending and authority matrices and delegations of authority, Written communications from the Chairman, President, CEO or Corporation to all or a group of members (if any), Contact information for officers and directors, Bi-Annual Statement of Information to Secretary of State, Annual Registration Form RRF-1 filed with Attorney General, Disaster Recovery, Business Continuation and Emergency Plans, Licenses and Certificates – Federal, State, Local)	A + 10 years	Business Reasons; Statute of Limitations
Contracts - General / Miscellaneous	**All Agreements and Contracts not otherwise addressed in another category of this Retention Schedule** (including letters, emails, etc. that constitute all or part of an agreement or which are important clarifications of an agreement)	A + 10 years	Business Reasons; Statute of Limitations
Corporate Policies	**Corporation's written policies** (e.g., Records Management and Retention, Acceptable Use of Technology, Email Disaster Recovery / Business Continuation, Emergency, IT Security, and Risk Management Plans)	A + 10 years	Business Reasons; Statute of Limitations
Mergers & Acquisitions (Excluding Agreements)	**Records relating to mergers, acquisitions, divestitures** (e.g., letters of intent, correspondence, due diligence)	A + 10 years	Business Reasons; Statute of Limitations

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
Agreements	**Agreements and contracts relating to structure of Corporation** (e.g., mergers and acquisitions, divestitures)	A + 10 years	Business Reasons; Statute of Limitations
Donor and Grant Records	**Records relating to donations and grants** (e.g., general donation records, grant proposals, grant agreements and modifications, grantee correspondence, grantee reports)	A + 10 years	Business Reasons; Statute of Limitations
Insurance Policies[4]	**Insurance policies insuring Corporation / Employees** (e.g., Commercial general liability, other liability, professional errors & omissions, property damage / hazard, workers compensation)	A + 10 years (potentially permanent)	Business Reasons; Statute of Limitations
HUMAN RESOURCES / PERSONNEL			
Benefit Plans	**Records evidencing or relating to employee benefits provided by Corporation** (e.g., health insurance plans, disability plans, defined benefit / contribution plans, retirement plans, pension plans; records of committee or fiduciary meetings; benefit statements and information; funding reports; disbursements; investment performance and earning reports; reports filed with Federal and State Agencies)	A + 10 years, including duration of Benefit Plan	29 U.S.C. §§ 1027, 1113, 1451 (ERISA) (6 years); 29 U.S.C. § 1059 (ERISA) (duration not specified); 26 U.S.C. § 6001 (duration not specified); Statute of Limitations
Trust, Fiduciary, Provider and Third-Party Administration Agreements	**Contracts or Agreement with third party administrators** involved in servicing Employee Benefit Plans	A + 10 years, including duration of Benefit Plan	Business Reasons; Statute of Limitations; 29 U.S.C. §§ 1027, 1113, 1451 (ERISA) (6 years); 29 U.S.C. § 1059 (ERISA) (duration not specified); 26 U.S.C. § 6001 (duration not specified)
Travel & Expense Reports	**Reports of employee travel and expenses**	C + 3 years	Business Reasons; Statute of Limitations
Employment Applications / Pre-Employment	**Records relating to employment applications and other pre- employment activities** (e.g., general job applications, resumes, employment advertising and solicitations). See Employee Personnel Files below for employee-specific records.	C + 3 years	29 CFR 1627.3 (ADEA) (3 years); 29 CFR 1602.14 (CRA) (3 years); Cal. Gov't. Code § 12946 (2 years)
Payroll Records	**Records relating to payroll and compensation to employees** (e.g., employee payroll and	Duration of employment + 4 years	26 CFR 31.6001-1 (IRS) (4 years); 29 CFR 1627.3 (ADEA) (3 years);

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
	compensation records including records with employee name, social security number, hours worked, compensation rate, deductions, total pay for pay period)		Cal. Lab. Code §§ 1174(d), 1197.5(d) (2 years)
Employment Actions Generally (Excluding Personnel File)	**Records relating to actions taken by Corporation concerning employment actions generally (not including specific employee records maintained in the personnel file)** (e.g., hiring, promotions, demotions, transfers, selection for training, disciplinary actions, layoffs, reductions in force, recalls, or other related employee actions). See Employee Personnel Files below for employee-specific records.	C + 4 years	29 CFR 1627.3 (ADEA) (3 years); 29 CFR 1602.14 (CRA) (1 year); Cal. Labor Code § 1198.5 (3 years); Statute of Limitations
Employee Personnel Files <u>EXCLUDING</u> Medical Records	**Records maintained in an employee's personnel file** (e.g., records relating to hiring, employment and termination, such as resumes, applications and related materials, employment offers, employment contracts, promotion, demotion, change of status, transfer, salary, separation, employment eligibility, I-9 forms, letters of recognition and/or commendation, disciplinary records, **<u>excluding</u>** medical records)	Duration of employment + 4 years	Business Reasons; Statute of Limitations; 29 CFR 1627.3 (ADEA) (3 years); Personnel Action Records – 1 year from when personnel action taken – 29 CFR 1627.3 (ADEA); 1 year from when personnel action taken or when record made, whichever is later 29 CFR 1602.14 (CRA)
Employee Health Condition and Medical Records	**Records relating to employee's health condition and medical treatments** (e.g., Workers' Compensation, Family and Medical Leave Act, the Americans with Disabilities Act, employment accommodations, leave of absence documents pertaining to an ADA accommodation, employment immunizations, drug screen information) <u>Medical records</u> to be stored separately in confidential and secure location.	Duration of employment + 30 years. (Except if employment < 1 year – records can be provided to employee; also does not include health insurance claims records maintained separately and first aid records (i.e., one-time treatment and observation of minor injuries) if maintained separately)	29 CFR 1910.1020 (OSHA) (30 years); 29 CFR 825.500 (3 years); 29 CFR 1630.14(c)(1)

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
Employee Exposure to Toxic or Hazardous Materials	**Records describing exposure to toxic or hazardous materials**, including the identity of the substance to which the employees were exposed plus information related to the methods used to determine the actual exposure; the identity of employees exposed; detailed environmental monitoring records and material safety sheets can be destroyed at an earlier period provided that adequate summary records are maintained. Medical records to be stored separately in confidential and secure location.	Duration of employment + 30 years. (Except if employment < 1 year – records can be provided to employee; also does not include health insurance claims records maintained separately and first aid records (i.e., one-time treatment and observation of minor injuries) if maintained separately)	29 CFR 1910.1020 (OSHA) (30 years); 29 CFR 825.500 (3 years); 29 CFR 1630.14(c)(1)
Employee Injury and Illness Logs	**OSHA Logs of Work-Related Injuries and Illnesses** and other logs, summaries and reports describing recordable cases of injury and illness, including the extent and severity of each case, and total injuries and illnesses. Medical records to be stored separately in confidential and secure location.	5 years following end of calendar year to which the records pertain	29 CFR 1904.33 (OSHA) (5 years); 29 CFR 825.500; 29 CFR 1630.14(c)(1)
Employment and Contractor Agreements	**Agreements and contracts with employees, independent contractors, consultants, etc.** (e.g., employment, change of control, non-compete, non-disclosure, temporary labor)	A + 10 years	Business Reasons; Statute of Limitations
HR-Related Agreements	**Agreements and contracts with third parties providing human relations / employment-related products or services** (e.g., recruiting / headhunter agreements, payroll companies, employee leasing)	A + 10 years	Business Reasons; Statute of Limitations
Employee Pension and Benefit Plans Excluding Agreements	**Plans and records relating to employee pension, retirement and benefit plans** (e.g., benefit, retirement, ERISA, and pension plans, and records relating to administration thereof)	A + 10 years, including duration of Benefit Plan	Statute of Limitations; 29 U.S.C. §§ 1027, 1113, 1451 (ERISA) (6 years); 29 U.S.C. § 1059 (ERISA) (duration not specified); 26 U.S.C. § 6001 (duration not specified)
Employee Pension and Benefit Plans Agreements	**Agreements relating to employee pension, retirement and benefit plans** (e.g., contracts and agreement with plan administrators, fiduciaries,	A + 10 years, including duration of Benefit Plan	Statute of Limitations; 29 U.S.C. §§ 1027, 1113, 1451 (ERISA) (6 years); 29 U.S.C. § 1059 (ERISA) (duration not specified); 26

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
	investment advisors, service providers)		U.S.C. § 6001 (duration not specified)
LEGAL			
Litigation Files	**Files relating to litigation involving Corporation** (e.g., investigations, pleadings, correspondence, research, invoices, settlement agreements)	A + 10 years	Business Reasons; Statute of Limitations
Claims (Litigation Not Filed)	**Claims, threats, demand letters, etc. where litigation not filed**	10 years after last correspondence or contact with claimant	Business Reasons; Statute of Limitations
Agreements	**Contracts and agreements retained in the Legal Department**	A + 10 years	Business Reasons; Statute of Limitations
Intellectual Property	**Records relating to intellectual property of Corporation** (e.g., copyright, trademark and patent applications and registrations, and related correspondence; license agreements)	Life of the intellectual property + 7 years	Business Reasons; Statute of Limitations
Government Filings subject to False Claims Act	**Records relating to filings with US Government** that could result in claims under the False Claims Act (e.g., requests for payment under government contracts or grants)	A + 10 years	31 U.S.C. 3731(b) (6 years); Statute of Limitations
FUNDRAISING MATERIALS / DEVELOPMENT DEPARTMENT RECORDS			
Advertising, Marketing and Public Relations Agreements	**Contracts and agreements for advertising, marketing and public relations products and services** (e.g., agreements with marketing and advertising firms, advertising contracts, directory advertising agreements, zip code coverage agreements)	A + 10 years	Business Reasons; Statute of Limitations
Advertising, Marketing and Public Relations Materials – Excluding Agreements	**Materials (excluding contracts) relating to Corporation's advertising, marketing and public relations activities** (e.g., advertisements, marketing collateral, catalogs, brochures, advertising copy, marketing programs, mailing lists, speeches and presentations, product literature)	A + 10 years	Business Reasons; Statute of Limitations
FACILITIES MANAGEMENT			
Furniture, Fixtures and Equipment (Excluding Contracts)	**Records relating to** Corporation's furniture, fixtures and equipment (e.g., asset lists, inventory lists, replacement schedules, maintenance and repairs, IT infrastructure and	C + 7 years	26 CFR 301.6501 (IRS) (6 years)

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
	architecture, telephone installation, fixed asset purchases)		
Furniture, Fixtures and Equipment – Contracts	**Contracts and agreements relating to Corporation's furniture, fixtures and equipment** (e.g., purchase, leasing and acquisition contracts; repair and maintenance contracts; warranty contracts; computer hardware and software licenses)	A + 10 years	Business Reasons; Statute of Limitations
Information Technology	**Records relating to Corporation's information technology systems** (e.g., software licenses; equipment purchase agreements; support, maintenance and warranty agreements; software inventories and audits; equipment inventories; IT policies)	A + 10 years	Business Reasons; Statute of Limitations
Property Tax Records	**Records relating to real estate and personal property taxes paid by Corporation**	A + 7 years	Business Reasons; Statute of Limitations
Property Acquisition / Ownership	**Records relating to acquisition and ownership of property** (e.g., deeds, leases, mortgages, construction)	Permanent	Business Reasons; Statute of Limitations
Agreements	**Contracts and agreements relating to operation and management of facilities** (e.g., property/facilities management agreements, repair/maintenance contracts, janitorial, landscaping)	A + 10 years	Business Reasons; Statute of Limitations
Hazardous/Environmental Contamination Removal	**Records regarding remediation / removal of environmentally contaminated or hazardous materials**	A + 30 years	29 CFR 1910.1020 (OSHA)
Hazardous / Environmental - Other	**Logs and other records regarding general compliance with OSHA and other environmental laws**	C + 5 years	Statute of Limitations; 3 years under Emergency Planning & Community Right-to-Know Act, Toxic Substances Control Act, Resource Conservation & Recovery Act, but advisable to keep longer due to potential liability concerns; 29 CFR 1904.33 (OSHA)
Certificates of Occupancy/Building Permits	**Certificates of Occupancy / Building Permits**	A + [10] years	Business Reasons; Statute of Limitations

FUNCTION	DESCRIPTION	RETENTION PERIOD	REFERENCE
SALES			
Sales Agreements	**Contracts and agreements relating to the sale of Corporation products and services**	A + 10 years	Business Reasons; Statute of Limitations
Sales Records	**Records other than contracts documenting sales of Corporation products and services** (e.g., invoices, receipts, credit card receipts, SKU details)	C + 10 years	Business Reasons; Statute of Limitations

[1] See Notes 1 and 10 to the Records Management and Retention Policy for reasons why it is important for a corporation that has such a policy to destroy records in conformity with the adopted retention schedule. It is important that a corporation adopting such a policy take care to identify on the schedule all record types that it will want to retain and not just use the list on this form policy without thinking through the record categories carefully.

[2] Examples of documents that are not included in the chart but may be relevant to various types of nonprofit organizations include the following, and will be subject to various regulatory requirements:

- Health care providers may be required to retain patient records, insurance and billing records, and records of compliance with health and safety regulations for specified periods.

- Organizations that have a license for a particular service (such as child care) may be required by the licensing agency to retain certain specified documents for a certain period of time, and may wish to retain other documents to prove their compliance with various licensing requirements in case of audit by the licensing agency.

- Organizations that work with children should be aware that the statute of limitations for a claim by a child may be tolled until the child reaches the age of maturity. As a result, organizations that work with children may wish to retain sign-in sheets or other proof of attendance, as well as any other records that would tend to show what had occurred on the premises, until several years past the date that the relevant children reach age 18, for the purpose of serving as proof of whether a particular child was in the organization's care on the date of any alleged harm.

[3] A corporation may have business reasons that require records to be retained for periods that differ from those set forth in the chart. Accordingly, each corporation should consider its own business issues and incorporate retention periods that are consistent with such practices.

[4] In determining whether an insurance policy is "active" or "inactive," it is important to look at the type of policy and when claims may be made under the policy. Some insurance policies are written on a "claims made" basis, meaning that the policy will cover only claims that are made to the insurance company during the year the policy is in force. Other policies are written on an "occurrence" basis, meaning that the policy covers claims made arising out of events or actions that occurred during the year the policy is in force. An "occurrence" basis policy therefore should be retained for as long as any claim could be made arising out of an event or action that occurred during the year covered by the policy. Care should be taken in determining the type of policy before determining whether a policy is inactive. A corporation's insurance company may require records be retained for periods that differ from those set forth in the chart. Accordingly, a corporation should also consult its insurance broker or company to confirm whether they have any specific requirements.

FORM OF RECORDS MANAGEMENT AND RETENTION POLICY FOR A CALIFORNIA NONPROFIT PUBLIC BENEFIT CORPORATION

* * *

APPENDIX A: FORM OF LEGAL HOLD NOTIFICATION

DATE:

TO:

CC:

FROM:

LEGAL HOLD

IN ACCORDANCE WITH [**NAME OF CORPORATION**]'S ("CORPORATION") RECORDS MANAGEMENT AND RETENTION POLICY, YOU ARE HEREBY NOTIFIED TO LOCATE AND PROTECT ALL RECORDS PERTAINING TO THE FOLLOWING SUBJECT MATTER:

_____

_____

_____

A LEGAL HOLD HAS BEEN PLACED ON RECORDS PERTAINING TO THE SUBJECT MATTER DESCRIBED ABOVE. YOU ARE REQUIRED TO LOCATE AND PROTECT THE NECESSARY RECORDS FOR WHICH YOU ARE RESPONSIBLE. ANY RECORD (INCLUDING BUT NOT LIMITED TO COMPUTER RECORDS, E-MAIL, VOICE MAIL MESSAGES, TEXT MESSAGES, INSTANT MESSAGES, HANDWRITINGS, PHOTOGRAPHS, PHOTOCOPIES, OR FACSIMILE) THAT IS RELEVANT TO THIS LEGAL HOLD MUST BE PRESERVED. FOR PURPOSES OF THIS LEGAL HOLD, TO "PRESERVE" ALSO MEANS TO SUSPEND FROM DELETION OR PROTECT FROM OVERWRITING, MODIFICATION OR DESTRUCTION. IF YOU ARE UNSURE WHETHER A RECORD IS RELEVANT TO THIS LEGAL HOLD, YOU SHOULD PROTECT THAT RECORD UNTIL YOU HAVE RECEIVED CLARIFICATION FROM [YOUR SUPERVISOR].

FAILURE TO COMPLY WITH THIS LEGAL HOLD WILL RESULT IN DISCIPLINARY ACTION, UP TO AND INCLUDING TERMINATION OF YOUR EMPLOYMENT OR OTHER SERVICE TO CORPORATION. IN ADDITION, FAILURE TO COMPLY WITH THIS LEGAL HOLD MAY RESULT IN FINES, DAMAGES, LIABILITY AND/OR COURT-ORDERED SANCTIONS IMPOSED AGAINST CORPORATION.

CONTACT THE FOLLOWING PERSON BY PHONE OR BY E-MAIL IF YOU HAVE ANY RECORDS SUBJECT TO THIS LEGAL HOLD:

Name: Phone: E-Mail:

CONTACT THE FOLLOWING PERSON BY PHONE OR BY E-MAIL SHOULD YOU BECOME AWARE OF ANY FAILURE TO COMPLY WITH CORPORATION'S RECORD MANAGEMENT AND RETENTION POLICY OR ANY LEGAL HOLD:

Name: Phone: E-Mail:

THIS LEGAL HOLD REMAINS EFFECTIVE UNTIL CORPORATION'S [LEGAL COUNSEL] [OR AN OFFICER OF CORPORATION] RELEASES IT IN WRITING. AFTER YOU RECEIVE WRITTEN NOTICE OF RELEASE, YOU MAY RETURN ALL RECORDS SUBJECT TO THIS LEGAL HOLD TO THEIR NORMAL RETENTION PROCEDURES.

CONTACT THE FOLLOWING PERSON BY PHONE OR BY E-MAIL FOR QUESTIONS REGARDING THIS LEGAL HOLD.

Name:_____ Phone:_____ E-Mail:_____

ACKNOWLEDGMENT OF LEGAL HOLD

I HAVE READ AND UNDERSTAND THE NOTICE OF LEGAL HOLD DATED [DATE] AND AGREE TO COMPLY WITH IT.

Name: _____

Signature: _____

Date: _____

APPENDIX B: FORM OF LEGAL HOLD RELEASE

DATE:

TO:

CC:

FROM:

LEGAL HOLD RELEASE

IN ACCORDANCE WITH CORPORATION'S RECORDS MANAGEMENT AND RETENTION POLICY, YOU ARE HEREBY NOTIFIED THAT THE LEGAL HOLD PERTAINING TO THE FOLLOWING SUBJECT MATTER:

_____

_____

_____

IS RELEASED. PLEASE RETURN ALL RECORDS RELEVANT TO THE LEGAL HOLD TO THEIR NORMAL RETENTION PROCEDURES [UNLESS SUBJECT TO ANOTHER LEGAL HOLD].[1]

CONTACT THE FOLLOWING PERSON BY PHONE OR BY E-MAIL FOR QUESTIONS REGARDING THIS LEGAL HOLD RELEASE:

Name: Phone: E-Mail:

[1] **Note:** A corporation with multiple legal holds may need to include this language if a document is subject to more than one legal hold.

APPENDIX C: ELECTRONIC COMMUNICATIONS POLICY

<u>Note</u>: This Electronic Communications Policy is a sample document containing relatively typical provisions and topics to be addressed in such a policy. Due to the vast differences in how different organizations operate and the legal requirements pertaining to Corporation, this sample will require modification and customization for appropriate use.

* * *

ELECTRONIC COMMUNICATIONS POLICY

OF

[NAME OF CORPORATION]

A California Nonprofit Public Benefit Corporation

ARTICLE I. GENERAL GUIDELINES

Section 1. **<u>Purpose / Scope</u>.** The purpose of this Electronic Communications Policy ("Policy") is to ensure the proper use of [**Name of Corporation**]'s ("Corporation") Electronic Communication systems and make employees, contractors, volunteers and other users ("Users") aware of what Corporation deems as acceptable and unacceptable use of its Electronic Communication systems or in using other permitted e-mail or electronic communications systems for conducting Corporation business. Corporation reserves the right to amend this Policy at its discretion. In case of amendments, Users will be informed appropriately. This Policy applies to e-mail, instant messages, text messages, PIN messages, chat and other electronic communications (collectively referred to as "Electronic Communications") used within Corporation and for Corporation business either now or in the future, and does not supersede any state or federal laws~~,~~ or any other Corporation policies regarding confidentiality, information dissemination, and standards of conduct. This policy is not intended to restrict communications or actions protected or required by state or federal law.

Section 2. **<u>Legal Risks</u>.** Electronic Communications are a business communication tool and Users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature Electronic Communications seem to be less formal than other written communication, the same rules apply. Therefore, it is important that Users are aware of the legal risks of Electronic Communications. For example, if you send Electronic Communications with any libelous, defamatory, offensive, racist or obscene remarks, you and Corporation can be held liable. If you forward confidential information of Corporation without authorization, Corporation can suffer significant losses, and you and Corporation can be held liable for violating third party confidentiality rights. Sending Electronic Communications with casual or informal language that can be taken out of context can be damaging to Corporation in the event of a lawsuit relating to the subject matter of the Electronic Communications. Electronic Communications may have to be disclosed in court proceedings or investigations by regulatory bodies, therefore, you must exercise good judgment, forethought and common sense when creating and distributing Electronic Communications. Accordingly, it is important for all Users to understand that the careless or

improper use of Electronic Communications can result in significant losses to Corporation, and potential liability of Corporation and User.

Section 3. **Ownership.** Corporation's e-mail system is the sole and exclusive property of Corporation. Any User files, e-mail, and other information stored on the e-mail system are the property of Corporation. Corporation may also store copies of such data and communications for a period of time after they are created, and may delete such copies from time to time without notice.

ARTICLE II. AUTHORIZED USE / RESTRICTIONS

Section 1. **Authorized Use.** You are authorized to use Corporation's e-mail system to lawfully conduct business for Corporation in accordance with this Policy and the other policies and rules of Corporation. Corporation's e-mail system constitutes a valuable business asset of Corporation and may only be used for approved purposes. Users are permitted access to the e-mail system to assist them in the performance of their jobs. This Policy's description of prohibited usage is not exhaustive, and it is within the discretion of Corporation to determine if there has been a violation.

Section 2. **Personal Use.** Occasional, limited, appropriate personal use of Electronic Communications is permitted when the use does not: (i) interfere with User's work performance; (ii) interfere with any other User's work performance; (iii) unduly impact the operation of the e-mail system; (iv) result in any material expense to Corporation; (v) violate any law or regulation of any jurisdiction; or (vi) violate any other provision of this Policy or any other policy, guideline, or standard of Corporation. Personal use of Electronic Communications is a privilege, not a right. Abuse of the privilege may result in appropriate disciplinary action. Users should keep in mind that all Electronic Communications are recorded and stored along with the source and destination. Users are prohibited from using Corporation's devices or their own personal devices to photograph, record, videotape, or otherwise capture any image or likeness of another User, their work space, or their property without their consent. In accordance with Article IV, management of Corporation has the ability and right to view Users' Electronic Communications.

Section 3. **Inappropriate or Unlawful Material.** Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, discriminatory, defamatory, or otherwise unlawful or inappropriate, including any comments that would offend someone on the basis of race, age, sex, sexual orientation, gender identity or expression, religion, political beliefs, national origin, marital status, medical condition, genetic information, veteran status, or disability, must not be sent by e-mail or other forms of electronic communication. In addition, unlicensed or unauthorized access to proprietary or copyrighted information is prohibited. Users encountering or receiving such material must immediately report the incident to their supervisor or other responsible manager. Because Electronic Communications can be inadvertently sent to unintended recipients, intercepted, obtained by third parties in litigation, and obtained by the government in investigations, before sending every Electronic Communication ask yourself if you would be comfortable with this Electronic Communication being publicly disclosed. If not, you should probably reword the Electronic Communication or communicate in a different manner, such as verbally.

Section 4. **Non-Corporation Business.** Users may not use the e-mail system for personal financial gain or the benefit of any third party (including the sale of any non-Corporation products or services), or to solicit others for activities unrelated to Corporation's business or sponsored activities, or in violation of Corporation policies and applicable laws relating to political activity or lobbying. The e-mail system may also not be used to create, store, or distribute any form of malicious software (e.g., viruses, worms, or other destructive code).

Section 5. **Excessive Use.** Users may not deliberately perform acts that waste Electronic Communications or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending non-business related mass e-mailings or chain e-mail, subscribing to a non-business related electronic mailing list, excessive use of e-mail for non-business related activities (e.g., personal purposes, playing games, engaging in non-business related online "chat groups"), or otherwise creating unnecessary network traffic.

ARTICLE III. PROPER USE OF ELECTRONIC COMMUNICATIONS

Section 1. **In General.** All User e-mail addresses assigned by Corporation and associated data and passwords shall remain the sole and exclusive property of Corporation. Users should endeavor to make each of their electronic communications truthful, accurate, and consistent with the qualities of good business communications. Always allow time to reflect before composing and sending a message. The following guidelines should be followed in drafting e-mail:

(a) Avoid using all capitals;
(b) Avoid excessive use of bold-faced type;
(c) Only mark truly high priority items as "Priority";
(d) Avoid copying unnecessary parties with the "Reply All" feature, particularly when individuals outside Corporation are addressees;
(e) Make the subject line for your e-mail descriptive;
(f) Avoid using graphic backgrounds for your e-mail and ornate type fonts. These will make your e-mail less readable and will require far greater company resources to store and transmit than ordinary e-mail; and
(g) Do not send messages to all users or other large groups within Corporation unless business related and a compelling business reason exists.

Section 2. **Altering Attribution Information.** Users may not alter the "From" line or other attribution of origin information in e-mail or other online postings. Anonymous or electronic communications sent using fictitious names are forbidden. However, a User many specifically grant another User the right to send Electronic Communications on behalf of the grantor (e.g., a manager authorizing her assistant to send an e-mail on her behalf).

Section 3. **Forwarding Electronic Communications.** Users should use their good judgment in forwarding Electronic Communications to any other person or entity. When in doubt, request the sender's permission before forwarding the message. Electronic Communications containing confidential information or attorney-client communications may never be forwarded without the permission of the sender or other authorized personnel. All messages written by others should be forwarded "as-is" and with no changes, except to the extent that the changes are clearly

indicated in the original text (e.g., by using brackets [ ] or different formatting to indicate changes to the text).

Section 4. **Confidential Information / Attorney-Client Communications.** Confidential information includes, but is not limited to, all information belonging to Corporation and not generally known, in spoken, printed, electronic or any form or medium, which was obtained from Corporation, or which was learned, discovered, developed, conceived, originated, or prepared by a User in the scope and course of employment, relating directly or indirectly to: business processes, practices, methods, policies, plans, publications, documents, research, operations, services, strategies, techniques, agreements, and contracts of Corporation or of any other person or entity that has entrusted information to Corporation in confidence. Confidential information also includes other information that is marked or otherwise identified as confidential or proprietary, or information that would otherwise appear to a reasonable person to be confidential or proprietary in the context and circumstances in which the information is known or used. Each User must take all appropriate precautions to insure that confidential information is not improperly disclosed or otherwise compromised. If confidential information is transmitted via Electronic Communication, the sender of the message is responsible for (i) ensuring the message is clearly labeled in the subject line and the body of the message as "Confidential," "Proprietary," "Confidential: Unauthorized Use or Disclosure is Strictly Prohibited" or "Privileged Attorney-Client Communication" for communications to or from in-house or outside counsel for Corporation, (ii) keeping the number of recipients to a minimum, (iii) ensuring all recipients are aware of the obligation to maintain the confidentiality of the information contained in the message, and (iv) assuring that the transmission of information is in accordance with this Policy and applicable law.

Section 5. **Receipt of Unsolicited, Unintentional, or Misdirected Confidential Information.** In the event a User receives an Electronic Communication, whether designated as confidential or not, by mistake, the User should stop reading the message and immediately notify the sender or system administrator. It is a violation of this Policy to read Electronic Communications intended for another person without the express prior consent of that person or other authorized Corporation personnel.

Section 6. **Electronic Mailing List Subscriptions.** Users should be selective in subscribing to electronic mailing lists, listserves and other e-mail distribution lists. Some discussion groups are very active and may result in dozens of e-mail every day. Promptly unsubscribe to any electronic mailing lists that are not business-related. When subscribing to an electronic mailing list, make sure to keep a record of the steps necessary to cancel the subscription. This information is usually contained in an initial message from the electronic mailing list, but may not be easily located later.

Section 7. **Access to E-mail Through Third Party Services.** Users must be authorized by an appropriate Corporation manager to use a home computer, PDA, tablet, laptop, cellular device, web mail, or a third party service to access their Corporation e-mail.[1] Users must

[1] Consider whether to include a Bring Your Own Device (BYOD) policy. If so, Corporation may incorporate a BYOD provision that allows employees to use their own electronic devices for work purposes. Conversely,

delete all copies of e-mail from the third party system within fourteen (14) days after receiving the e-mail. The transmission of a User's business related e-mail to a third party e-mail service provider or account maintained by User must be infrequent, irregular, and temporary and must be done to accomplish a specific business purpose. Users may not use alternate, non-Corporation provided or authorized e-mail addresses to directly receive business related e-mail.

Section 8. **Retention and Destruction of Electronic Communications.** Users may not use their e-mail account as a long-term repository for records. [If applicable, insert Electronic Communications deletion policy, e.g., delete after ninety (90) days; limits on e-mail storage, etc.] Users should not store Electronic Communications on the individual hard disks of their workstations or make backup copies of the Electronic Communications independent from those created and maintained by Corporation. Each User is responsible for ensuring that their use of Electronic Communications is consistent with this Policy and Corporation's Records Management and Retention Policy. If a permanent or lasting record is required of any Electronic Communication, the User shall print the Electronic Communication and retain it in accordance with Corporation's Records Management and Retention Policy. Electronic Communications maintained by a User in violation of this Policy or Corporation's Records Management and Retention Policy may be automatically deleted by authorized personnel without advance warning. Users may not circumvent storage prohibitions by sending, forwarding, or copying any Electronic Communication or related documents to themselves or others for the purpose of evading this requirement.

ARTICLE IV. NO EXPECTATION OF PRIVACY

Section 1. **Monitoring of Electronic Communications and Internet Usage.** All of Corporation's information systems and the content of such systems are the property of Corporation. Users do not have a right to expect that any information that they place, transmit, or receive on these systems is private. Corporation maintains the right and the ability to monitor, retrieve, read, and publish all messages and documents sent, received, composed, and/or stored on these information systems. In addition, Corporation monitors Internet usage including websites accessed and information downloaded. Although User passwords may be required for access to these information systems, use of these passwords does not guarantee privacy or confidentiality. Users should not place any messages or documents on these information systems that, if disclosed, will be embarrassing to the User, the receiver, or Corporation. A User's use of and access to these information systems may be monitored by management at any time, even after files, data, or messages appear to have been deleted by the User or even after the User's employment has been terminated. All Users should structure their electronic communications in recognition of the fact that Corporation and third parties may, from time to time, have the need to examine their content or use. Corporation may also store copies of such data and communications for a period of time after they are created, and may delete such copies from time to time without notice.

Section 2. **User Names or Passwords.** Notwithstanding Corporation's right to monitor its information systems, Users who are issued or who create passwords for these information systems are responsible for protecting their own passwords from misuse. Users are not to give out their

Corporation may draft a stand-alone BYOD Policy detailing which personal devices are permitted as well as security requirements and appropriate use guidelines for personal devices.

information systems' passwords to other personnel without a valid business reason. All user names, passwords, and information used or stored on Corporation's information systems are the property of Corporation and Corporation may override a User's password for any reason. Any User who knows or suspects that any user name or password has been improperly shared or used, or that this Policy has been violated in any way, must report that suspicion to their supervisor or other responsible manager. Failure to report such breach of access may result in disciplinary action.

ARTICLE V. DELETION AND RETENTION OF ELECTRONIC COMMUNICATIONS

Section 1. [Insert Corporation's e-mail deletion policy as appropriate (e.g., Corporation will automatically delete e-mails older than sixty (60) days or will delete e-mails in Outlook Sent folder after six (6) months).]

Section 2. Each User must determine if an Electronic Communication should be retained under Corporation's Records Management and Retention Policy in a manner to ensure Electronic Communications are not automatically deleted as describe above. Corporation's approved Retention Schedule, attached to the Records Management and Retention Policy, identifies categories and types of records to be retained and the retention period for each category. It is the content and function of an Electronic Communication that determines the retention period for that message. All Electronic Communications sent or received by a Corporation employee or volunteer in the scope or course of Corporation business is considered a Corporation record. Therefore, all Electronic Communications must be retained or disposed of according to Corporation's Retention Schedule.

Section 3. It is the responsibility of the User of the e-mail system, with guidance and training from Corporation's employee responsible for records management, to manage e-mail messages according to Corporation's Retention Schedule. It is the responsibility of the sender of e-mail messages within Corporation's e-mail system and recipients of messages from outside Corporation to retain the messages for the approved retention period. Names of sender, recipient, date/time of the message, as well as any attachments must be retained with the message. The preferred method for retaining e-mails is through the use of Personal Folders using Corporation's Microsoft Outlook application (see instructions below or contact the Information Technology Department for assistance).[2] Printing and appropriate filing of e-mails is also permitted~~,~~ but not encouraged due to the loss of ability for electronic searching.

Section 4. Electronic Communications stored electronically should only be stored in Outlook Personal Folders on Corporation's networked servers [identify server name / location if desired], and not on computer hard drives, local drives, CD-ROMs, floppy disks, flash drives, thumb drives or other removable media.

Section 5. Personal Folders using Outlook can be created as follows:

(a) Open Outlook
(b) Click on "File"

[2] This sentence should be revised to match Corporation's preferred or required method for archiving e-mails.

(c) Click on "Account Settings"
(d) Click on "Data Files"
(e) Click on the "Add" button
(f) This box allows you to designate the drive and folder you want your e-mail to go to. It will default to the Outlook folder. You might want to direct it instead to a folder on Corporation's server you have created. Once you designate the folder (at the top of the text box), then name the file that your e-mails will reside in and click "OK" or "Apply" whichever is listed.
(g) Now your personal file should appear on the left-hand column of your Outlook screen. You can add subdirectories to this (just like you would with the "Inbox").[3]

Section 6. Each User must comply with the legal hold requirements of Corporation's Records Management and Retention Policy for retention of records, including e-mails, in the event of pending, threatened or reasonably foreseeable claims, litigation or investigations. Users must also fully cooperate with supervisors or Corporation management in responding to legal and Corporation requests for Electronic Communications which are or may be relevant to a claim, litigation or investigation.

ARTICLE VI. THIRD PARTY E-MAIL PROVIDERS

Unless expressly authorized by an appropriate supervisor or manager, you should not use third party e-mail providers such as your home or personal e-mail account or web-based e-mail providers (e.g., Yahoo, Google, etc.) for sending or receiving e-mails pertaining to Corporation business.

ARTICLE VII. VIOLATIONS

A violation of this Policy may result in disciplinary action, up to and including termination of employment, as well as potential civil and criminal liability. You agree to assist Corporation in investigating any potential or actual violations of this Policy.

[3] Revise and customize this language to be consistent with Corporation's preferred or required method for archiving e-mails.

APPENDIX D: REMOVAL FROM STORAGE RECORD

Description of Record(s):

Identification of Box or Receptacle:

Person Removing Record

Name:
Department:
Location:
Telephone No:

Purpose for Removal:

Record is Confidential: _____ No _____ Yes

(If yes, describe method of determining clearance and authorization)

Date Removed:

Date of Scheduled Return:

Date of Actual Return:

Signature of Personnel Removing Record	Signature of Custodian
Printed	Printed
Date	Date