RMOUG's mission

RMOUG's mission is an independent, non-profit organization formed to empower its members with the best education in database, application, development and personal networking opportunities in the Rocky Mountain Area and beyond.

This Policy's Purpose

The purpose of this Document management, retention, and destruction (DMRD) policy is to assist the RMOUG Board of Directors in effectively managing the important documents of the organization. Future volunteers and members of the organization will need the documentation generated to aid with future decisions, and as a tax-exempt non-profit charity, the organization is required to retain and have available certain documents at all times. Likewise, since the retention of documents is a cost and a burden to the organization, this policy will determine when it is safe to destroy documents. Any changes to this investment policy will be made in writing and communicated to all parties.

Document Management

Although organizational documents may originate from a variety of sources (i.e. emails, social media postings, privately-held documents, etc), this policy will provide guidance on how the organization will store documents of importance.

The basic principle is that the organization will retain and store soft-copies of important documents whenever possible. If a document originates as hard-copy, then it will be digitized into electronic media (such as PDF format) as soon as possible. If there is no legal reason to retain the hard-copy in addition to the electronic copy, then the hard-copy will be shredded and discarded soon after it is digitized. If the hard-copy must also be retained, then it will stored in appropriate archive-quality files and stored in an environment where the risk of damage is minimal.

Important organizational documents on electronic media will be archived on read-only media redundantly, so that there is always at least two copies on separate storage media.

The organization will retain shared storage accessible to all members of the board of directors and the executive director. Important documents will be stored in this shared storage in a folder structure similar to the "Basic Infrastructure Checklist" described in the Colorado Nonprofit Association's PDF of the same name at http://www.coloradononprofits.org/wp-content/uploads/2011BasicInfrastructureChecklist.pdf.

In other words, the root folder for all RMOUG documents will contain the following folders representing the basic infrastructure checklist for a non-profit organization…

- Governance & Leadership
- Transparency & Accountability
- Financial Management
- Fundraising
- Human Resources
- Planning
- Evaluation
- Advocacy & Civic Engagement
- Communications

- Information Technology
- Strategic Alliances

The intent is that the organization's documentation should be organized to facilitate an audit by anyone familiar with the principles of the Colorado Non-profit Association, and that our documentation should be organized according to these principles as well.

1. Policy and Purposes

This Policy represents the policy of RMOUG (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 president 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