Maharashtra Foundation, Inc.

Document Retention Policy

This policy outlines the guidelines for retaining and disposing of documents and records for the Maharashtra Foundation, Inc. It applies to all physical and electronic documents, including emails, created, received, or maintained by board members, officers, employees, and volunteers in the course of their duties.

Purpose

The purpose of this policy is to:

- Ensure compliance with legal and regulatory requirements.
- Preserve essential records necessary for the operation and history of the Maharashtra Foundation.
- Minimize risks associated with improper document destruction or retention.
- Promote efficiency in record management.

General Principles

- **Legal Compliance:** All document retention and destruction will comply with applicable federal, state, and local laws and regulations, including those specific to 501(c)(3) non-profit organizations.
- **Confidentiality:** Documents containing sensitive or confidential information will be handled and disposed of securely to protect privacy.
- **Accessibility:** Retained documents will be stored in an organized manner to ensure easy retrieval when needed.
- **Good Faith:** This policy is to be followed in good faith. No document should be destroyed if there is any ongoing or anticipated litigation, audit, investigation, or subpoena related to that document.

Document Categories and Retention Periods

The following table outlines the minimum retention periods for various types of documents. In some cases, legal requirements may dictate longer retention periods than those listed here.

Document Category	Examples	Retention Period
Corporate & Legal Records	Articles of Incorporation, Bylaws, IRS determination letters (501(c)(3) status), Board meeting minutes, Resolutions, Legal correspondence, Contracts, MOUs, Copyrights, Trademarks, Insurance policies, Audits (external), Annual reports to regulatory bodies (e.g., state Attorney General), Intellectual Property documentation.	**Permanently**
Financial Records	Audited financial statements, IRS Form 990s, General ledgers, Journals, Bank statements, Canceled checks, Deposit slips, Accounts payable/receivable ledgers, Budgets, Grant agreements (signed and completed), Grant reports (final), Receipts, Invoices, Expense reports, Payroll records (including tax forms like W-2s, 1099s), Donation records (donor names, addresses, donation amounts, acknowledgment letters).	**7 Years**
Human Resources Records	Employee personnel files (hiring, performance reviews, compensation, disciplinary actions, termination), Employment applications (for hired individuals), I-9 forms, Payroll records (detailed, separate from summary financial), Benefits enrollment and	**7 Years after Termination** or **7 Years (Payroll)**

Document Category	Examples	Retention Period
	claims, Health and safety records, Training records.	
Program & Project Records	Project proposals (funded), Program reports (interim and final), Evaluation reports, Beneficiary data (ensure privacy compliance), Partnership agreements, Photographs and media related to programs, Volunteer agreements and records.	**7 Years**
Grant & Fundraising Records	Grant applications (submitted and rejected), Donor cultivation records, Fundraising campaign materials, Gift agreements (if not permanent corporate), Donor communication (general).	**7 Years**
Operational Records	Administrative policies and procedures, Internal communications (significant), Equipment maintenance records, IT system documentation, Vendor contracts (non-program specific), General correspondence.	**3-7 Years**
Temporary/Draft Documents	Drafts of documents, preliminary notes, internal memos with no long-term significance, duplicate copies, general announcements, outdated lists.	**Until no longer needed (daily/weekly/monthly)**

Document Storage

- **Physical Documents:** Stored in secure, organized filing systems in designated office areas. Access should be limited to authorized personnel.
- **Electronic Documents:** Stored on secure servers with regular backups. Access should be password-protected and restricted to authorized personnel. Cloud storage solutions must be vetted for security and compliance.
- **Confidentiality:** Documents containing sensitive information (e.g., donor details, financial data, personnel records) must be stored with enhanced security measures.

Document Destruction

- **Scheduled Destruction:** Documents that have met their minimum retention period will be reviewed for destruction.
- **Secure Disposal:**
    - **Physical Documents:** Sensitive documents will be shredded or incinerated. Non-sensitive documents can be recycled.
    - **Electronic Documents:** Electronic records will be securely deleted from all storage locations, including backups, ensuring they are unrecoverable.
- **Documentation of Destruction:** A log will be maintained documenting the date, type of documents destroyed, and the method of destruction.

Responsibilities

- **Board of Directors:** Responsible for approving and overseeing the implementation of this policy.
- **Executive Director:** Responsible for ensuring the overall implementation and adherence to this policy.
- **Designated Staff/Compliance Officer:** Responsible for managing the document retention schedule, overseeing proper storage and destruction, and acting as the point of contact for questions regarding this policy.
- **All Staff, Officers, and Volunteers:** Responsible for understanding and adhering to this policy in their daily activities.

Policy Review

This policy will be reviewed by the Board of Directors at least **every three years** or as needed to ensure compliance with changing legal requirements and organizational needs.

Policy approved by the Board of Directors on Aug 20, 2025.