



DOCUMENT RETENTION AND DESTRUCTION POLICY

1. Policy and Purposes

This Policy represents the policy of Tucson Amateur Astronomy Association (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 Board of Directors is responsible for the thoughtful retention of its key documents and the Board will task the TAAA Secretary to be the administrator (“Administrator”) in charge of this Policy. The Administrator shall make best efforts to include supervising and coordinating both 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 to retain such documentation. 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, and maintaining control of the documents. The Administrator will ensure that, at all times, the Executive Committee of the Board of Directors has knowledge of how to access all documents.

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 and leaders 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 over which they have temporary physical control upon request of the Administrator or 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, the administrator will make a best effort 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). A list of all documents the volunteer retained will be promptly provided to the Administrator by the volunteer and checked by the Administrator. 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~~ stressing the importance of compliance. A Volunteer who does not comply with the Document Retention Policy may not continue to serve in any volunteer role in TAAA until he/she does comply with the Document Retention Policy. Noncompliance must be reported by the Administrator to the Board.

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. 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, they shall promptly 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.

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. It should be noted, however, that all key documents of TAAA will be maintained in both an electronic and a paper format and that the electronic and paper versions will always be stored in different locations. Electronic versions may be reviewed and updated periodically to ensure continued availability.

5. Privacy. The Administrator will utilize best effort, including use of outside counsel, if needed, to determine how privacy laws will apply to the organization’s documents from and with respect to employees (if such exist) and other constituencies; to establish reasonable procedures for compliance with such privacy laws; and to allow for document audit and review on a regular basis. The Administrator shall keep a record of such efforts.

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, for updating of electronic formats, and for permanent retention in different locations of both paper and electronic copies of key TAAA documents. Documents will be stored in a manner that includes appropriate temperature and environmental protections. Locked access of documents (whether physical or electronic) will be provided with limited, approved access.

7. Document Creation and Generation. The Administrator shall make best efforts to discuss with Board Members, volunteers, contractors, and membership the ways in which documents are created, generated, stored and/or destroyed and shall document those efforts. With respect to each 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. Ideally, the organization will create and archive documents in a way that facilitated identification and destruction of documents with similar expirations. When needed, the Administrator may acquire the expertise of an archivist librarian to facilitate organization of the document collection.

8. Document Retention Schedule.

<u>Document Type</u>	<u>Retention Period</u>
Accounting and Finance	
Accounts Payable	5 years
Accounts Receivable	5 years
Annual Financial Statements and Audit Reports	Permanent
Bank Statements, Reconciliations & Deposit Slips	5 years
Canceled Checks – routine	5 years
Canceled Checks – special, such as loan repayment	Permanent
Credit Card Receipts	5 years
General Ledger	Permanent
Semi Annual Financial Statements	5 years
Contributions/Gifts/Grants	
Contribution Records and grant Requirements	Permanent
Documents Evidencing Terms of Gifts	Permanent
Grant Records	5 years after end of grant period
Corporate and Exemption	
Articles of Incorporation and Amendments	Permanent
Bylaws and Amendments	Permanent
Minutes, including Board & Executive Committee Minutes	Permanent
Annual Reports to Secretary of State	Permanent
Other Corporate Filings	Permanent
IRS Exemption Application (Form 1023 or 1024)	Permanent
IRS Exemption Determination Letter	Permanent
Permits and Licenses	Permanent
Employer Identification (EIN) Designation	Permanent

Electronic Mail (E-mail) to or from the organization

TAAA is at present an all-volunteer organization without corporate email, and, thus, retaining volunteers' personal emails related to TAAA is not reasonable or feasible. Should TAAA in the future hire personnel, then this should be reconsidered.

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 also be retained in hard copy form (unless the electronic aspect is of significance).

Documents are retained in Cloud Storage on Microsoft Onedrive.com (or other such Cloud Storage service) by username tucsonastronomy@hotmail.com. Ability to access and make changes in such documents will be controlled by the Administrator in coordination with the Board.

Insurance

Property, D&O, Workers' Compensation and General Liability Insurance Policies	10 years
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	5 years after expiration
Policies and Procedures	Current version with revision Date – Permanent until revised

Property – Real, Personal and Intellectual

Property deeds and purchase/sale agreements	Permanent
Property Tax	Permanent
Property Leases	5 years after termination
Trademarks, Copyrights and Patents	Permanent

Tax

Tax exemption documents & correspondence	Permanent
IRS Rulings	Permanent
Annual information returns – federal & state	5 years after filing
Tax returns	5 years after filing