Policy #: Record Retention and Destruction

Governed by: Administration

Approval Date: March 7, 2022 **Last Updated:** March 7, 2022

Purpose: To ensure the systematic review, retention, and destruction of records received or created by agency staff in the course of conducting business.

The Agency retains and maintains agency Records, as defined herein, in accordance with this policy and federal and state laws governing record retention and record destruction.

Records often contain information that has an enduring business value such as where the Record provides a record of a business transaction, evidences the Agency's rights or obligations, protects the Agency's legal interests, or ensures operational continuity. Such records can be in electronic or paper form.

The accidental or intentional destruction of these Records during the retention period, specified in the Record Retention Chart, could result in consequences to include fines, penalties; loss of legal rights and privileges that the Records may evidence and help preserve; inference of spoliation of evidence; and/or reputational damage.

Therefore, this policy is part of an agency-wide system for the review, retention, and destruction of records that the Agency creates or receives in the course of its operations. The goals of this policy are to:

1) Retain important business documents in electronic format for reference and future use;
2) Delete documents that are no longer necessary for the proper functioning of the Agency;
3) Organize important documents for efficient retrieval; and
4) Ensure that Agency employees, know what documents should be retained, the length of their retention, means of storage, and when and how they should be destroyed.

Retention of Records:

Record: A record is any type of physical or electronic document, file, or material that contains information related to agency business, staff, or transaction received, transmitted, or created during any business-related transaction. Records may include:

- Contracts
- Emails
- Fundraising and donor information
- Audio and video recordings
- Handwritten notes
- Invoices
- Online postings on social media platforms and websites
- Letters and other correspondence

A non-exhaustive list of such records and their retention requirements are set forth in the Record

Retention Chart. The information listed in the chart is intended only as a guideline and may not contain all records the Agency may be required to retain in the future.

Documents received electronically are a part of this policy and must be retained or deleted in accordance with the Record Retention Chart.

Email: Staff are encouraged to regularly review and manage their email accounts by deleting junk or non-pertinent emails to free up valuable storage space. Active user accounts will only maintain access to emails from the previous 12 months. If the user has a sufficient reason to retain an e-mail message in their mailbox beyond the 12-month time frame, such message should be copied in an appropriate file on the Agency's computer system or be printed in hard copy and retained in an appropriate file.

Staff who send or receive email communication containing sensitive data, such as social security number, driver's license or non-driver identification numbers, account numbers, or biometric information, are required to follow the process for sensitive data in compliance with the NY SHIELD Act. After securing any sensitive data received via email, the staff can delete the email from their user account; however, it will automatically delete within 12 months.

Review of Records and Destruction:
On an annual basis, the Human Resources Manager will be responsible to initiate structured document review and destruction activities throughout the Agency. At that time, all Program Directors will organize the review of records within their respective departments to identify any records or documents that are eligible for destruction as outlined in Appendix 1. If deemed necessary, program staff may conduct record reviews and destruction activities following an alternative schedule with their Program Director's approval.

Data Backup:

Daily backups are created and stored initially on a local Datto appliance and then immediately after backup to the local appliance, copies of those backups are transmitted to two offsite Datto data centers in the United States. The offsite backups are encrypted during transmission and at rest. Datto employs end-to-end AES 256-bit encryption with SSL key-based encryption to secure data. Additionally, Datto's data center backup servers require long and complex passwords and multi-factor authentication (MFA).

Disposable Information:
Generally, "Disposable Information" is information in any form that would normally be a Record, except that it:

- Serves a temporary useful purpose or no purpose;
- Is no longer required for the operation of the Agency; and
- Is not required by law or this policy to be retained by the Agency

Examples may include:

- Duplicates of originals that have not been annotated;
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record;
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the Agency and retained primarily for reference purposes; and
- Spam and junk mail.

Disposable Information may be safely destroyed without violating this policy.

Correspondence:

Correspondence should be retained for the same period as the document it pertains to or supports. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration); however, an email or letter that references the contract but offers no additional information can be discarded.

Routine letters, memos, meeting minutes, etc. relating to any matters that **do not** pertain to documents having a prescribed retention period should be discarded after 12 months. However, those pertaining to non-routine matters or having significant lasting consequences or directly relating to a current staff member must be retained with the associated documents/files and follow the associated retention requirement.

Destruction/Deletion

Tangible Records

Tangible records should be destroyed by shredding or some other means that will render them unreadable. If an employee does not know how to destroy a record, such as a photograph, compact disc, or tape recording, they should consult with HR Manager.

Electronic Records

Electronic records should be deleted from local devices by deleting the file and then emptying the trash, recycling bin, or deleted items folder. To delete electronic records from the shared network, consult with the IT Administrator who will delete the file or folder and can confirm that the deleted file has been removed from the network.

The agency's electronic destruction procedure for devices includes wiping of the device and then physical destruction of the hard drive by a third party vendor.

Off-site backup data is not and cannot be deleted.

Cessation of Record Destruction/Deletion

If a lawsuit is filed or imminent, the Agency is the subject of an investigation or audit, or a legal document request has been made upon the Agency, all record destruction concerning that activity must cease immediately. Failure to adhere to comply with this section may result in fines and penalties, among other disciplinary actions.