



Autoimmune Registry Inc. Document Destruction and Retention Policy

1. Purpose:

The purpose of this Document Destruction and Retention Policy is to ensure the proper management, retention, and secure destruction of documents and records maintained by Autoimmune Registry Inc. (hereinafter referred to as "the Organization"). This policy is designed to facilitate compliance with legal requirements, safeguard sensitive information, and manage storage space efficiently.

2. Scope:

This policy applies to all employees, volunteers, contractors, and board members associated with Autoimmune Registry Inc.

3. Document Categories:

- a. Administrative Records:
 - Includes documents related to general administrative activities, such as human resources, finance, and organizational operations.
- b. Programmatic Records:
 - Encompasses documents related to the programs, projects, and initiatives undertaken by the Organization.
- c. Legal and Compliance Records:
 - Involves documents related to legal matters, contracts, compliance, and regulatory requirements.
- d. Financial Records:
 - Includes documents related to financial transactions, budgets, audits, and tax records.

4. Document Retention Periods:

- a. Administrative Records:
 - Retained for a minimum of 7 years after the end of the fiscal year.
- b. Programmatic Records:
 - Retained for a minimum of 5 years after the completion of the program or project.
- c. Legal and Compliance Records:
 - Retained for a minimum of 7 years or as required by applicable laws.
- d. Financial Records:
 - Retained for a minimum of 7 years after the end of the fiscal year or as required by the relevant regulatory agencies.

5. Document Destruction:

- a. Regular Review:
 - A designated records custodian will conduct regular reviews to identify records that have met their retention period.
- b. Secure Destruction:
 - Documents scheduled for destruction will be securely shredded, deleted, or otherwise rendered unreadable to protect sensitive information.



6. Exceptions:

Certain documents may be subject to longer retention periods due to legal or regulatory requirements, pending audits, investigations, or other exceptional circumstances. In such cases, the records custodian will document the reasons for the extended retention.

7. Record Custodian:

The Chief Data Officer (or if the Chief Data Officer is unavailable, then the Executive Director) is designated as the responsible party for overseeing the implementation of this policy and coordinating the secure destruction of documents.

8. Training and Awareness:

All employees, volunteers, contractors, and board members will receive training on this policy to ensure understanding and compliance.

9. Review and Revision:

This policy will be reviewed periodically and updated as necessary to reflect changes in legal requirements or organizational needs.