

# Academic Preservation Trust Preservation Policy, Version 3.1

[DOI: 10.18130/sw8m-dp84](https://doi.org/10.18130/sw8m-dp84)

## Scope and Objectives

This policy describes APTrust's preservation components in our repository, which are available to all Academic Preservation Trust (APTrust) member organizations. It applies to all content members deposited into the APTrust environment in all storage classes. The APTrust [Mission Statement](#) guides this policy.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

## Policy statement

Preservation services, components, and strategies are described by storage class. All storage classes share some elements; these are described first.

## Shared Preservation Services, Components, and Strategies

1. Content is preserved in its original format.
  - 1.1. Deposited content will be rebagged when restored, according to the current APTrust BagIt Profile and BagIt Specification, but no changes will be made to the data.
  - 1.2. Content will be owned, updated, and deleted solely by the depositor.
  - 1.3. Deposited content MUST NOT contain sensitive or personally identifying information unless encrypted.
    - 1.3.1. It is the member's responsibility to manage their encryption keys.
  - 1.4. Content is deposited at the member's own risk.
2. Bit-level object preservation.
  - 2.1. APTrust performs fixity checks on every file during ingest and restoration to ensure data integrity.
  - 2.2. Depositors can use MD5 or SHA256 algorithms when depositing content.

- 2.2.1. APTrust will calculate fixity using multiple checksum algorithms, including cryptographically secure algorithms.
        - 2.2.1.1. To prevent a bad actor from translating the fixity value into the original file.
        - 2.2.1.2. To make it unlikely or impossible for someone to replace a valid file with an invalid one that produces the same fixity value.
    - 2.3. Internal alerts notify APTrust staff when a fixity check fails, and advisory representatives are emailed to be informed.
3. Access.
  - 3.1. Authentication and authorization are documented in our Trusted Digital Repository documentation.
    - 3.1.1. Members can use Multi-Factor Authentication for logging into the preservation repository.
    - 3.1.2. Multi-factor deletion prevents the destruction of data by a single bad actor.
4. Metadata, search, and discovery.
  - 4.1. APTrust provides members with a web interface for the preservation repository.
  - 4.2. APTrust also provides a member API and Partner Tools for members to search and discover content in the preservation repository.
  - 4.3. APTrust does not index metadata outside the requirements in the APTrust BagIt Profile.
5. Preservation events and logging.
  - 5.1. APTrust records preservation events as PREMIS metadata attached to intellectual objects.
    - 5.1.1. These events include creation (within the APTrust repository), identifier assignment, ingestion, access assignment, fixity, restoration, and deletion.
    - 5.1.2. Members can retrieve PREMIS event metadata through the member API.
  - 5.2. APTrust maintains lower-level logs across all infrastructure for system integrity.
6. Object management.
  - 6.1. APTrust maintains a basic relationship among objects in an external metadata store managed by the repository.
  - 6.2. All preservation files are tagged (at the underlying object storage level) with metadata essential for valid restoration.
    - 6.2.1. These metadata properties include depositing institution, intellectual object name, file identifier, and original MD5 and SHA256 checksums.
7. Restoration
  - 7.1. APTrust members can restore content using multiple methods.
    - 7.1.1. Individual object restoration through the repository web interface.
    - 7.1.2. Individual file restoration through the repository web interface.

- 7.1.3. Bulk object restoration can be done by authorized request to APTrust staff.
- 7.2. Members can enable restoration spot tests at a frequency of their choosing by request.
  - 7.2.1. Restoration spot tests perform automated object restorations on a fixed schedule so members can test local restoration procedures.
- 8. Service enhancements
  - 8.1. APTrust is a member organization. Features and enhancements will be developed based on user input and member requests.
  - 8.2. There is no formal schedule for new releases; they are deployed on a rolling basis.

## High Assurance Storage Class

- 9. Geographic storage diversity.
  - 9.1. APTrust stores one (1) copy on the East Coast (Virginia) and one (1) copy on the West Coast (Oregon).
- 10. Technical storage diversity.
  - 10.1. East Coast copies are in hot storage, and West Coast copies are in cold storage.
    - 10.1.1. While APTrust cannot assert which technologies the underlying storage providers use for hot and cold storage, we know they are different.
- 11. Enhanced bit-level object preservation
  - 11.1. APTrust performs recurring fixity checks of hot copies every 180 days to ensure data integrity.
  - 11.2. When a file fails a fixity check, APTrust retrieves the cold copy and verifies fixity before replacing the corrupted hot copy.

## Basic and Deep Archive Storage Classes

Content in the Basic Archive and Deep Archive storage classes does not have enhanced preservation services but has characteristics worth noting.

- 12. Geographic storage diversity.
  - 12.1. APTrust stores one (1) copy in a location specified by the depositor: East Coast (Virginia), Mid-West (Ohio), or West Coast (Oregon).
- 13. Technical storage diversity.
  - 13.1. Basic Archive storage uses cold storage technology.
  - 13.2. Deep Archive storage uses frozen storage technology.

## Related policies and documents

- [APTrust User Guide](#)
- [APTrust Preservation Services User Guide](#)
- [APTrust Preservation and Storage](#)
- [APTrust Storage Fact Sheet](#)
- [APTrust Trusted Digital Repository documentation](#)

## Further information

[BagIt File Packaging Format Specification](#)

[NDSA Fixity Best Practices](#)

[NDSA Fixity Survey](#)

[PREMIS \(Preservation Metadata\)](#)

## Definitions

Term	Definition
Cold Storage	Data that can be accessed within 1-12 hours of the request.
Fixity	Verifying that an object has not been inadvertently changed, adapted, or corrupted
Frozen Storage	Data that can be accessed within 12-48 hours of request.
Hot Storage	Data that can be accessed instantly from its storage location.
PII	Personally Identifiable Information (e.g., Social Security Numbers)
Depositor	An entity that has been authorized to put materials into the APTrust environment

## Roles and stakeholders

Roles	Responsibilities
APTrust Staff	Responsible for the technical details of this policy.
Advisory Committee	Responsible for approving any new versions of this policy.
Governing Board	Responsible for final approval of any new version of this policy.

## Review

Review frequency: Every 2 years or when new service options are added

Next review date: January 2027

## Version History

Version	Status	Date	Notes
.1	Done	1/12/17	Comments from APTrust Community
.2	Done	2/9/17	Communications Group approves vote for APTrust
.7	Done	3/16/17	APTrust Advisory Committee approval
.8	Done	3/17/17	Minor edits completed based on Advisory Feedback
1.0	Done	4/2018	Board Vote and Approval - <a href="#">DOI</a> uploaded
1.1	Done	11/2019	Open for comments from APTrust Community
1.8	Done	10/2020	Advisory Committee Vote
2.0	Done	10/2021	Board Vote and Approval - <a href="#">DOI</a> uploaded
3.0	Done	10/22 - 10/24	APTrust staff and the Advisory Committee reviewed and revised this document for accuracy. Language about six copies in the high-assurance (standard) storage class was removed. The policy now reflects all storage classes instead of only the high-assurance (standard) class. Title changed to drop "Core". The Advisory Committee approved.
3.1	Done	January 2025	Board review for approval and <a href="#">DOI</a> obtained.