Academic Preservation Trust
Core Preservation Service Policy

Scope

This policy sets out the current preservation-service components offered by the Academic Preservation Trust [APTrust] in its core, high-assurance preservation service. The policy applies to all content that members deposit into the APTrust environment via the tools and ingest policies set down in our basic operating principles. This policy is guided by the APTrust Mission Statement.

Objectives

This policy outlines the core preservation activities that each depositor can expect to receive from APTrust. It is broken down into three parts. The Administrative section indicates the frequency and responsible party for updating the policy; the Content section outlines the parameters of responsibility; and the Service section details the services and commitments provided to APTrust users.

Policy statement

1. **Administrative**
    1.1. This policy is to be reviewed and updated annually by a group designated by either the APTrust Board and/or the Advisory Committee.
2. **Content**
    2.1. Content is preserved in its original format (guided by the these goals)
        2.1.1. Materials deposited will be rebagged but no other changes to the individual files will be undertaken by APTrust staff/services
        2.1.2. Content will be managed solely by the depositor
        2.1.3. APTrust Community is currently requested not to submit any content that is known to have PII or other types of privacy or contractual restrictions [This policy is currently not enforced and will be superseded by Access Policy when it is complete].
3. **Service Components**
    These are the particular elements (benchmarks) for preservation in APTrust's core, high-assurance computing? service.
    3.1. Bit level object preservation
        3.1.1. APTrust staff are notified when a failure occurs. and a copy from the secondary storage repository. Glacier in Oregon is used to replace the corrupt copy.
            3.1.1.1. Future phase will notify the depositor of this action.
        3.1.2. Fixity checks will be performed on every file
            3.1.2.1. Cryptographically secure
            3.1.2.2. Frequency
                3.1.2.2.1. Current frequency is every 90 days per file.
            3.1.2.3. Based on cost for frequency (i.e. if less than or greater than 90 days)
    3.2. Geographical diversity of content storage (East and West coast)
        3.2.1. APTrust stores one (1) copy in Amazon Web Services (AWS) in Northern Virginia and one (1) copy in Glacier in Oregon. Internally, S3 and Glacier each have 3 copies of that file, totalling 6 overall.

3.3. Multiple storage technologies

3.3.1. Two different storage technologies

3.3.1.1. S3 (spinning disk)

3.3.1.2. Glacier [technology not announced by AWS, but not spinning disk]

3.4. Multiple Checksums

3.4.1. Using both SHA256 and MD5

3.4.1.1. Partner generates the MD5 (on submission) and APTrust generates the SHA256

3.4.2. AWS uses eTag for receipt of transfer

3.4.3. MD5 Checksum of any file downloaded from AWS

3.5. Appropriate access (authentication and authorization is documented as part of our TDR work particularly section 4.6.1)

3.6. Search and discovery of metadata

3.7. Logging of all preservation actions

3.7.1. Register of PREMIS events based on the Library of Congress standard

3.7.1.1. Auditing of PREMIS events (we capture and put locally)

3.7.1.2. Lower level logs of activities for system integrity

3.7.1.3. S3 Generates logs as part its architecture that we can capture

3.7.1.4. Able to copy those logs to local storage logs

3.8. Data syncing across storage layers

3.9. Standardized metadata set (the current elements agreed upon by partners)

3.10. APTrust maintains a basic relationship among objects contributed by a partner

3.10.1. Though the more robust version of this is managed locally

3.11. Content Retrieval

3.11.1. Batch downloading (i.e. by the bag)

3.12. Ongoing Development

3.12.1. Updating the APTrust environment is ongoing. Based on user input and requests new services are added as needed. There is no formal schedule for revising and updating--it is continuous.

Related policies and subordinate documents

APTrust Mission Statement

Collection Development Policy

Preservation and Storage within APtrust

NOTE: Other items may be added to this section without requiring policy revision

Further information

NDSA Fixity Best Practices

NOTE: Other items may be added to this section without requiring policy revision

Definitions

Term	Definition
Fixity	Verifying that an object has not been inadvertently changed, adapted, or corrupted
PII	Personally Identifiable Information (e.g. Social Security Numbers)

Roles and stakeholders

- APTrust staff is responsible for updating the technical Services section of this document and vetting for accuracy. Each significant update will require a new version of this policy.
- APTrust Advisory Group is responsible for approving any new versions of this document.

Role/stakeholder	Responsibilities
Advisory Committee	Review entire document as needed but no less than annually
APTrust Technical Staff	Review and update Services (Section 3) as needed - at a minimum annually

Review

Review frequency: Annual
Next review date: January 2018

Version History

Version	Status	Date	Notes
.1	Done	1/12/17	Comments from APTrust Community ended
.2	Done	2/9/17	Communications Group approves vote for APTrust Community
.3	Done	3/16/17	APTrust Advisory Community approval
.35	Done	3/17/17	Minor edits completed based on Advisory Feedback
1.0	Done	4/2018	Board Approval