APTrust Preservation Storage Criteria

Executive Overview

This document synthesizes the results of the MoSCoW prioritization exercise conducted by the APTrust Preservation Storage Criteria Task Force, with additional feedback gathered from members at the Fall 2025 Member Meeting. It provides a comprehensive, community-informed set of requirements for preservation storage that balances security, transparency, and trustworthiness with practicality, sustainability, and long-term scalability.

The feedback reaffirmed strong priorities around **security**, **transparency**, and **resilience**, while identifying secondary priorities in **integration**, **documentation**, and **sustainability**.

Prioritization Summary

Must Have	Should Have	Could Have	Would Have
Encryption in transit & at rest	Transparency and reporting on stored content	Authentication integration (SSO)	—
Access controls to prevent unauthorized use	Documented content and infrastructure history	Integration with external preservation tools	—
Data integrity verification and fixity validation	Recovery and repair from the provider	Active fixity or external integrity checking	—
Physical media protection	Environmental sustainability and energy reporting	Discoverability features	—
Vendor reliability and reputation	ISO 27001 alignment (not certification requirement)	Automation of preservation actions	—

Key Themes from Member Feedback

1. Security and Confidentiality

- Universal agreement that encryption and secure transmission are non-negotiable.
- Staff and members emphasized the **Confidentiality–Integrity–Availability (CIA)** framework.
- Growing importance of supporting **PII and other sensitive data**.
- ISO 27001 is seen as an aspirational benchmark rather than a hard requirement.

2. Transparency and Accountability

- Desire for visibility into data operations, including:
    - Geographical storage location transparency.
    - Tracking of object status, fixity, and preservation events.
    - Clear reporting on file counts, bag size, and data transfer logs.
- Vendor transparency in pricing and incident communication is vital.

3. Trust and Vendor Reputation

- Preference for vendors with a proven track record and peer adoption in higher education.
- Institutions want confirmation that APTrust is not an early adopter of untested solutions.

4. Integration and Access

- **SSO integration**, in alignment with institutional IT trends, should be elevated to a higher priority for APTrust.
- Improved **search** and data retrieval workflows are essential.
- The ability to move or restore data via systems integrations is helpful but not a dealbreaker.

5. Environmental and Ethical Responsibility

- Sustainability is important, though its practical impact is modest compared to larger IT infrastructures.
- It remains a "Should Have" unless a future provider's footprint is significantly worse than that of APTrust's current providers.

6. Resilience and Recovery

- Emphasis on provider accountability for data recovery and integrity.
- Providers must **notify APTrust of any storage issues**.
- Demonstrable plans for **disaster recovery and fixity assurance**.

Finalized Criteria and Requirements

Must Have (Baseline Requirements)

1. **Encryption and Data Protection**
    - End-to-end encryption in transit and at rest.
    - Controlled access for content.
2. **Integrity and Fixity**
    - Periodic fixity checks with verification reporting.
    - Verified, permanent deletion, and checksum tracking.
3. **Resilience**
    - Provider must notify APTrust of storage integrity or availability issues.
    - Support for recovery and repair processes.
4. **Transparency**
    - Access to metadata and audit logs showing where and how data is stored.
    - Geographical awareness of data storage locations.
5. **Vendor Reputation**
    - Established reliability and peer trust through public adoption and audits.

Should Have (Enhanced Capabilities)

1. **Single Sign-On Integration**
    - Federated authentication for APTrust members to *receiving* and *restoration* buckets.
2. **Reporting and Metrics**
    - Granular reporting on file counts, sizes, and transfers.
3. **Documentation and Standards**
    - Internal documentation of infrastructure and content history.
    - ISO 27001 alignment where feasible.
4. **Sustainability and Environmental Impact**
    - Transparency in energy use and sustainability practices.
5. **Pricing Transparency**
    - Clear cost models and visibility into provider pricing structures.

Could Have (Future Enhancements)

1. **Automation**
    - Automated preservation actions (fixity re-checks, format migrations).
2. **External Integration**
    - Compatibility with preservation registries or external services.
3. **Discoverability**
    - Internal search or indexing tools for better data management.
4. **Active Fixity Validation**
    - Provider-led validation mechanisms beyond static checksum checks.

Summary Statement

Member input confirmed that APTrust's preservation storage priorities remain well-aligned with community expectations. **Security, transparency, and trustworthiness** are central and non-negotiable.

Future development should focus on improving **integration**, **documentation**, and **sustainability**, not just as compliance tasks, but as elements that reinforce APTrust's long-term stewardship mission and service accountability.

Preservation Storage Evaluation Rubric

This rubric provides a scoring guide to evaluate a storage provider against the final criteria prioritized by the APTrust Preservation Storage Criteria Task Force and member feedback.

Criteria Category	Requirement	Evaluation Level 3 (Fully Meets)	Evaluation Level 2 (Partially Meets)	Evaluation Level 1 (Does Not Meet)
Must Have (Baselin...	**Encryption and Data Protection** (End-to-end encryption in transit and at rest, Controlled access)	Fully compliant: provides and enforces end-to-end encryption and strong access controls.	Compliant with one (e.g., at-rest encryption only) or uses non-standard/uncontrolled access.	Does not provide encryption or lacks essential access controls.
Must Have (Baselin...	**Integrity and Fixity** (Periodic fixity checks with verification reporting, Verified permanent deletion, Checksum tracking)	Fully compliant: performs and reports on periodic fixity checks, with verified deletion and checksum tracking.	Performs some fixity/integrity actions but lacks comprehensive reporting or fails on verified deletion.	Provides no internal mechanism for fixity checks, verification, or guaranteed deletion.
Must Have (Baselin...	**Resilience** (Provider must notify APTrust of storage issues, Support for recovery and repair processes)	Fully compliant: has demonstrable recovery/repair processes and guaranteed notification of all issues.	Recovery/repair processes are documented but not fully tested, or notification is not immediate/comprehensive.	No defined or demonstrable plan for provider-led recovery, repair, or issue notification.

Must Have (Baselin…	**Transparency** (Access to metadata and audit logs, Geographical awareness of storage locations)	Fully compliant: provides clear, auditable logs and metadata, and exposes specific storage locations.	Logs/metadata are provided but are difficult to access, incomplete, or geographical location is general (e.g., "US").	Vendor does not provide access to audit logs or does not disclose data storage geography.
Must Have (Baselin…	**Vendor Reputation** (Established reliability and peer trust through public adoption and audits)	Fully compliant: has a stable, verifiable track record with peer adoption in higher education/archives.	Track record is established, but lacks significant adoption by peer organizations or clear audit results.	Is a new or unproven provider, or lacks transparent public track record/audits.
Should Have (Enha…	**Single Sign-On Integration** (Federated authentication)	Fully implemented: offers a production-ready, federated SSO solution for access.	SSO is planned, in beta, or only partially implemented for certain functions/buckets.	No plan or capability for SSO integration.
Should Have (Enha…	**Reporting and Metrics** (Granular reporting on file counts, sizes, and transfers)	Provides granular, easily accessible, and customizable reports and metrics.	Provides some basic reporting, but it is not granular, easily customizable, or access is difficult.	Only provides basic, high-level metrics (e.g., total capacity used).

Should Have (Enha…	**Documentation and Standards** (Internal documentation of infrastructure and content history, ISO 27001 alignment)	Excellent, current, and public/accessible documentation; clear alignment with ISO 27001 principles.	Documentation exists but is incomplete or outdated; has no formal alignment with ISO 27001.	Documentation is sparse or non-existent; no mention of industry security standards.
Should Have (Enha…	**Sustainability and Environmental Impact** (Transparency in energy use and sustainability practices)	Publishes clear, actionable reports on energy use and commitment to environmental sustainability.	Has general statements on sustainability but no specific metrics or transparent reporting.	Does not provide any information on energy use or environmental practices.
Should Have (Enha…	**Pricing Transparency** (Clear cost models and visibility into provider pricing structures)	Provides clear, predictable, and fully transparent cost models and pricing structures.	Cost models are complex or have hidden/variable fees that require detailed analysis.	Pricing is opaque, non-standardized, or subject to frequent, undisclosed changes.
Could Have (Future…	**Automation** (Automated preservation actions)	Fully implemented: provides automated actions like fixity re-checks and format migrations.	Provides tools for automation, but they require significant APTrust development/configuration.	No support for automated preservation actions.

Could Have (Future...	**External Integration** (Compatibility with preservation registries or external services)	Supports robust, current compatibility with external preservation registries or services.	Integration is planned, or only compatible with a limited/legacy set of external services.	No known or planned external service integration.
Could Have (Future...	**Discoverability** (Internal search or indexing tools)	Provides highly effective, internal search and indexing tools for better data management.	Basic search/indexing exists but is limited in scope or functionality.	No internal search or discoverability features.
Could Have (Future...	**Active Fixity Validation** (Provider-led validation beyond static checksum checks)	Implements active, provider-led fixity validation mechanisms.	Fixity is passive (e.g., on-demand or static checksum only).	Relies solely on APTrust for fixity validation.