-->

Data Retention and Disposal Standard

Last Modified on 05/18/2026 2:52 pm EDT

For more details about the Information Security Office, **please visit our website**!

1. Introduction

The Wharton Data Retention Standard defines the activities, responsibilities, and requirements for retaining, storing, and disposing of institutional data across Wharton-managed systems and services. Consistent data retention practices ensure Wharton complies with University and Wharton policies, legal/regulatory requirements, contractual obligations, and information security best practices.

This Standard establishes expectations for determining retention periods, managing data throughout its lifecycle, ensuring timely disposal, and documenting retention-related decisions.

1.1 Standard Owner

Wharton ISO is accountable for the development and maintenance of this Standard, in alignment with University policy, Wharton Information Security Policy, governance directives, and applicable laws and regulations.

System and data owners are responsible for implementing and documenting retention practices for the data they manage. Documentation must be available for audit upon request from ISO. ISO is available for consultation on any retention and disposal processes in development by system and data owners.

1.2 Purpose

The purpose of this Standard is to ensure that Wharton retains institutional data appropriately and disposes of it securely and consistently. This Standard promotes:

- Compliance with University policies, legal/regulatory requirements, and data classification standards.
- Transparency of data retention practices.
- Consistent application of minimum and maximum data retention periods.
- Secure disposal and minimization of long-term storage risks.
- Documentation that supports regulatory audits, legal holds, and governance reviews.

1.3 Scope

This Standard applies to:

- All Wharton-managed data, regardless of format (digital, physical, etc.).
- All faculty, staff, contractors, temporary personnel, and third-party service providers handling Wharton

data.

- All systems storing, processing, or transmitting Wharton institutional data, including cloud-based platforms under Wharton or University contract.

1.4 Compliance

This Standard aligns with University records retention policies, applicable regulatory requirements (e.g., FERPA, HIPAA, financial record regulations), and information security best practices (e.g., NIST).

All stakeholders must follow this Standard when determining data retention periods, storing institutional data, and performing data disposal.

1.5 Key Roles & Responsibilities

Role	Responsibilities
Data Owner	Identifies retention requirements for data sets under their authority. Ensures compliance with legal/regulatory mandates. Approves retention schedules.
System Owner	Ensures technical ability to retain and dispose of data according to approved schedules. Maintains documentation and supports audits.
University Archives & Record Center	Provides authoritative guidance on University-mandated retention schedules and archival requirements. Advises on archival procedures and long-term preservation. Under Penn's archival and records management policy, most Confidential records destruction is arranged and directed by University Archives.
Wharton ISO	Advises on secure storage and disposal methods. Confirms alignment with data classification requirements. Maintains this Standard.
Administrative, Academic, and Research Units	Apply approved retention schedules, ensure staff follow retention requirements, and manage operational execution.
Third-Party Service Providers	Must comply with Wharton and University retention and disposal requirements contractually and operationally.

2. Data Retention Requirements

Wharton-managed data must be retained only as long as required for business, legal, regulatory, or contractual needs. Retention periods must align with University Archives guidance wherever applicable, otherwise be documented and approved by the department/center.

2.1 Retention Schedules

Retention periods fall into the following categories:

- **Permanent/Archival:** Required for historical, legal, governance, or accreditation purposes.
- **Fixed-Term Retention:** Retained for a set time period based on policy, law, or operational need.
- **Event-Driven Retention:** Triggered by an event such as contract expiration, employee separation, or project closure.
- **Minimal Retention:** Retain only as long as operationally required or required by law, contract, policy, regulation, etc. then dispose promptly.

Authoritative retention schedules are published and maintained by the University Archives & Record Center, available here:
https://archives.upenn.edu/records-center/resources/retention-schedules/

Retention schedules must align with University standards (above), regulatory requirements, grant rules, and contractual obligations.

2.2 Data Classification & Retention Mapping

Retention requirements must align with Penn and Wharton data classification levels. Sensitive and critical data (e.g., Confidential) may require shorter retention periods to minimize risk unless legal requirements necessitate longer retention.

2.3 Legal Holds

A legal hold requires the preservation of relevant records beyond the scheduled retention period. ISO should be notified of any legal holds, investigations, etc. The following requirements apply:

- Only the Office of General Counsel (OGC) can initiate or release a legal hold.
- Upon initiation of a legal hold, system and data owners must suspend all deletion or destruction processes for affected records.
- Records subject to a legal hold may not be altered, deleted, or otherwise disposed of until the hold is formally released by OGC.

Suspension Due to Legal Process, Claims, or Investigations
In addition to formal legal holds, existing retention periods are suspended:

- Upon service of legal process (subpoena, summons, or similar),
- Upon learning of an investigation or audit,
- If a claim is made (formal or informal), or
- If a dispute arises, **the applicable record retention schedule must be suspended immediately**, and any related records must not be destroyed under any circumstances until the matter is fully resolved and the hold is lifted by OGC or the University's designated authority.

2.4 System Logging Retention

Logs generated by Wharton-managed systems must follow minimum retention requirements based on security and compliance purposes:

- **Security logs:** Retention should be as agreed upon and documented through a Risk Review, in accordance with the Wharton Logging Standard, or a default of 60 days given the absence of other guidance.
- **Application/system logs:** Additional logs beyond the minimal required. Identified and documented by system owner and available for audit upon request from ISO.

3. Secure Storage & Disposal Requirements

3.1 Secure Storage

Data must be stored in systems that meet Wharton and University security requirements for its classification level. Retention requirements do not supersede required security controls.

3.2 Secure Disposal

At the end of an approved retention period, data must be disposed of securely using methods appropriate to its format and classification.

Acceptable disposal methods include:

- Secure digital deletion with cryptographic erasure
- Physical destruction of media
- Document shredding
- Vendor-assisted destruction, where contractually appropriate

Confidential records disposal must be coordinated with the University Archives & Record Center to ensure fully compliant destruction procedures.

All disposal must be:

- Documented
- Approved by the Data Owner
- Logged in system or departmental records
- Irreversible and permanent

3.3 Disposal Failures & Exceptions

If disposal is not technically feasible, Wharton ISO should be consulted and an exception documented. Access to the data must be restricted using compensating controls.

4. Documentation & Review

Retention schedules, disposal events, and exceptions must be documented and retained for audit purposes. Documentation must include:

- Data set description
- Retention period and rationale
- Stakeholders or owning department
- Disposal date and method
- Exception requests, if applicable

Retention schedules must be reviewed at least every three years, or sooner if legal, regulatory, or business requirements change.

Where an existing retention period is documented for like categorization of data, that period should be held to absent a conflicting requirement. Given a conflicting requirement the retention should be modified to meet needs and document the deviation from the existing standard.

5. Compliance & Enforcement

All Wharton faculty, staff, contractors, and third-party providers must comply with this Standard. Failure to comply (including improper disposal, excessive retention, or retention of unapproved data) will be reviewed by Wharton ISO and may result in corrective actions, up to and including revocation of system privileges, mandatory retraining, or escalation through University governance.