Records Management Policy

Effective Date:	December 8, 2022
Supersedes:	Record Management Policy Effective December 26, 2014
Policy Review Date:	To be reviewed every 3 Years from effective date
Issuing Authority:	Research Foundation President
Responsible Party:	Chief Compliance Officer
Contact Information:	518-434-7145
	rfcompliance@rfsuny.org

Reason for Policy

All organizations need efficient and cost-effective methods to organize and maintain their records and information, and efficient record management is a key activity necessary to achieve the Research Foundation for The State University of New York's ("Research Foundation" or "RF") strategic goal of providing outstanding sponsored program administration services and stewardship to the SUNY community and sponsors. This policy is based upon standards rooted in federal and state laws and regulations, and an acknowledgment that contracts may obligate the RF to unique record management responsibilities. Legal and regulatory sources were used to identify the minimum requirements for specific types of RF Records.

Statement of Policy

RF Records must be managed in accordance with the RF Record Retention Schedules. Operating locations that choose to use and maintain Electronic Records must establish procedures that provide for the:

- creation and use of Electronic Records;
- security of Electronic Records;
- selection and maintenance of alternate storage mediums; and
- retention, disposition, and destruction, of Electronic Records.

RF Records should be destroyed when the retention requirement has been met, unless:

- there is a relevant audit, claim, or litigation pending or anticipated, or a preservation or production directive is in effect for the relevant Records; or
- a sponsor requires Records to be retained for a longer period, in which case the sponsor's requirements take precedence and must be followed.

Questions regarding the retention period for a specific document or class of documents not included in a Record Retention Schedule should be addressed to the Office of Compliance Services.

Research-Related Records that are not RF Records

Research-related Records in the custody, possession, or control of a SUNY campus are subject to SUNY policies and procedures, including but not limited to the State University of New York Records Retention and Disposition Policy. RF operations managers may elect to adopt the RF's policy to govern the management of research-related Records at their location, in conformance with local rulemaking procedures.

Electronic Records

Creation and Use of Electronic Records

Operating locations that maintain the Office of Record copy of documents must establish a procedure to implement the use of Electronic Records in substitution for original Records. The procedures *must* ensure:

- the process maintains the integrity of the original Records, is reliable and secure, and that authenticity can be validated;
- the image process preserves accurate images of original Records - including signatures, worksheets, relevant notes, and other papers necessary to reconstruct and understand the original Record;
- the index system provides secure, on-time, and convenient access and retrieval of imaged Records (i.e., each document should be identified sufficiently to enable authorized personnel to retrieve, protect, and carry out disposition of the document in the system.); and
- the transfer and disposition of Electronic Records maintain the integrity, reliability, and security of the original Electronic Records; and that a description of the transfer is maintained for audit purpose.

Security of Electronic Records

Operating locations *must* establish an effective Electronic Records security procedure to:

- ensure that only appropriate, authorized personnel have access to Electronic Records;
- provide for the backup and recovery of Electronic Records as protection against information loss;
- ensure that appropriate, authorized personnel are trained to protect sensitive, proprietary, or classified Electronic Records;
- minimize the risk of unauthorized alteration or erasure of Electronic Records;
- document that similar kinds of electronic generated/stored Records were created by the same processes each time, and have a standard method for retrieval;
- prevent the unauthorized change of an Electronic Record and ensure protection against system problems (e.g., power interruptions); and
- identify the electronic medium for Electronic Record storage throughout the lifecycle, and the maximum time that Electronic Records remain on each storage medium.

Selection and Maintenance of Alternate Storage Medium

Operating locations must select appropriate alternate mediums and systems for storing Electronic Records throughout the retention period. The mediums and systems *must*:

- provide for secure, on-time, and convenient Electronic Record access and retrieval;
- retain Electronic Records in a usable format until the authorized disposition date;
- ensure Electronic Records are not lost because of changing technology, portability of the medium (i.e., use with different hardware/software), and transfer to a different medium (e.g., magnetic tape to optical disk);
- store microfilm in a safe physical environment and in a fireproof cabinet to ensure safety of the Electronic Records; and
- provide adequate microfilm readers that produce legible close-to-original size paper copies of reproduction quality.

In addition, written procedures must be developed for the care and handling of direct access storage mediums that include any recommendations from the manufacturer.

Retention, Disposition and Destruction of Electronic Records

Operating locations must retain, dispose, and destroy Electronic Records according to the Records Management Policy and RF Record Retention Schedule(s), and must apply additional considerations for Electronic Records. The additional considerations include :

- the establishment of procedures for regular disposition (e.g., recopying, reformatting, other necessary maintenance) to ensure the use and retention of Electronic Records throughout the lifecycle;
- the identification of sensitive, proprietary, or classified information prior to the destruction of Electronic Records; and
- previously used electronic mediums *must* not be reused if the previously recorded information (e.g., sensitive, proprietary, classified) can be compromised by reuse in any way.

Responsibilities

The following table outlines the responsibilities for compliance with this policy:

Responsible Party	Responsibility
Department Heads	Have an understanding of what Records they create and/or receive and are required to manage.
RF Chief Compliance Officer	Manage and maintain RF Records where the Office of Compliance Services is the Office of Record.

	Monitor compliance across the enterprise under the purview of the owners identified below. Can suspend normal Record retention process pursuant to pending internal investigation.
RF Vice President of Human Resources	Manage and maintain RF Records in accordance with the Person-Related Record Retention Schedule and where the Office of Record is Human Resources.
RF Vice President, Sponsored Programs & Regulatory Affairs	Manage and maintain RF Records in accordance with the Project Administration Record Retention Schedule and where the Office of Record is Sponsored Programs.
RF Chief Financial Officer	Manage and maintain RF Records in accordance with the Account Expenditure Record Retention Schedule and where the Office of Record is Finance.
RF Vice President for Internal Audit	Manage and maintain RF Records where the Office of Record is Internal Audit.
RF Vice President, Industry and External Affairs	Manage and maintain RF Records in accordance with the Technology Transfer Record Retention Schedule and where the Office of Record is Industry and External Affairs.
RF General Counsel	Manage and maintain RF Records where the Office of Record is the Office of General Counsel. Can suspend normal Record retention process pursuant to pending investigation.
RF Operations Managers or designee	Manage and maintain Records in accordance with RF Record Retention Schedule(s) and where the campus is the Office of Record. Adopt and ensure compliance with this policy or the local policy and procedure for the management of research-related Records.

Definitions

Record(s) - Any information kept, held, filed, produced, or reproduced in any form whatsoever, including electronic, by or on behalf of the Research Foundation or Research Foundation employees, in their capacity as employees of the Research Foundation. Records include, but are not limited to: reports; statements; examinations; memoranda; opinions; folders; files; books; manuals; pamphlets; forms; papers; designs; drawings; maps; photos; letters; microfilms; computer tapes or discs; rules; and regulations or codes, in connection with the transaction of Research Foundation business.

Electronic Record(s) - Any information recorded in a format that requires a computer or other electronic device to access it and that otherwise satisfies the definition of a Record

RF Record(s)- Any Record in the custody, possession or control of the RF.

RF Record Retention Schedule - A document that prescribes the required minimum retention periods for Research Foundation Records.

Office of Record - The office responsible for maintaining a Record or an official copy of a Record

Related Information
Record Access Policy

Record Retention: Account Expenditure Records

Record Retention: Person-related Records

Record Retention: Project Administration Records

[Record Retention: Technology Transfer Records](#)

[Record Retention: Destruction of Records Guideline](#)

Forms
None

Change History

Date	Summary of Change
December 8, 2022	Revised pursuant to current RF corporate business practices for records management. Moved the previously-separate Electronic Records Policy into this policy.
February 18, 2022	Added link to new Destruction of Records Guideline.
December 26, 2014	Changed OMB reference to 2 CFR Part 200.