

Standard: Record Retention and Disposal

Information Security Standards

Record Retention and Disposal

Standard #	RRD-A	Effective Date	2/15/2016	Email	security@sjsu.edu
Version	4.0	Contact	Mike Cook	Phone	408-924-1705

Revision History

Date	Action
2/2/2016	Publication

Table of Contents

Introduction and Purpose 4

Scope 4

Standard of Practice 4

 Structure of oversight and stewardship of University records and data management: 5

 Types of University Records..... 5

 Retention of Records 6

 Cautions Regarding Disposal..... 6

 Disposal of Records 7

 Records Management Procedures : Annual reviews 7

 Definitions..... 7

Introduction and Purpose

[CSU Executive Order 1031](#) provides for the implementation of the California State University (CSU) systemwide records/information retention schedules to assist campuses in establishing appropriate operational best practices to meet their commitment to an effective records management program. This executive order requires every campus to develop and implement an Information Retention Management Standards.

San Jose State University (SJSU) creates, receives, uses, and retains records of its business processes and activities and the retention of these records are critical for the support of the university mission and its operations. An effective information retention program ensures that records are retain long enough to satisfy internal and external requirements, but not so long as to incur unnecessary storage and maintenance costs, protect unnecessary records from unauthorized access or expose the university to possible liability risks

Scope

This Standard of Practice addresses the retention and disposal of University records in hard copy, Transparent Film (includes Microfilm/Microfiche) and electronic formats. It applies to all divisions, departments and academic units of SJSU.

The Institutional Data Management Council will coordinate campus-wide communication and training on Retention Procedures. The first cycle of campus annual review of records for retention/disposal will start mid-October 2016.

This Standard is to be posted on the SJSU Information Security website <http://its.sjsu.edu/services/info-security/> along with all relevant instructions and guidelines.

Standard

Many University records are required to be retained for specific periods of time, taking into account legal or other institutional requirements. The records retention requirements for San Jose State University are set forth in the [CSU Record Retention and Disposal Schedules](#).

These schedules are the minimum retention periods required by the University. At the conclusion of the retention period, the records should be properly disposed of under this Standard. Requests to deviate from or modify this Standard or these retention periods must be made to and approved by the appropriate University Data Steward (See Appendix A).

University records and data are the property of the University and not of the officers, faculty members, or employees who create them or to whom they are entrusted.

Because the University is a State agency, University records and data are in fact State assets and must be safeguarded by all employees just like other kinds of assets.

This Standard sets forth procedures to ensure that the University:

- meets legal standards;
- properly manages the use of electronic and physical storage space;
- preserves the history of the University;

- disposes of outdated records.

No one person or unit can be directly responsible for all University Records. Therefore, every office or department storing University records is responsible for:

- Implementing records management practices consistent with this Standard.
- Educating staff in the Records management practices.
- Preserving Records as required under this Standard.
- Properly disposing of Inactive Records at the end of the applicable retention period.
- Protecting Records against misuse, misplacement, damage, destruction, or theft.
- Monitoring compliance with this Standard.

Structure of oversight and stewardship of University records and data management:

- CFO is the campus oversight for this function.
- The Institutional Data Management Council members serve as the principal officers for this function.
 - Information Security Office shall serve as a custodian for campus inventories of main repositories of data/records.
 - Departments are responsible for providing annual updates of repositories of data/records to Information Security Office.
- Director of Internal Control is the principal advisor for Administration.
- Each Data Steward shall serve as the principal advisor for their respective area. See Appendix A.
- Campus MPP's are responsible for compliance with this Standard within their areas. As fiduciaries of State assets, all MPP's have the responsibility to safeguard state assets in the category of official records and data. In particular,
 - Division VPs, Director of Athletics, President's Chief of Staff.
 - Directors on the Admin/Business side, Deans and Department Chairs on the Academic side.
 - Executive Directors of auxiliary organizations.

Types of University Records

Record: Any type of record created or received in the course of University business, including, but not limited to, paper, email, any type of electronic file or data, still photographs (including microfilm/microfiche), motion pictures, drawings, plans/blueprints, and audio/video recordings, etc.

- An **Active Record** is any Record that is currently in active use by an office or function of the University.
- A Record with **Personally Identifying Information** is a Record that includes an individual's name or personal mark together with that individual's Social Security Number, Drivers' License number or other government identification card number (excludes SJSU ID), financial account number or any number or code which may be used alone or in conjunction with another piece of information to assume the identity of another person, access financial resources, or obtain credit information. Personal Information is highly sensitive and must be safeguarded and secured at all times.
- An **Archival Record** is an Inactive Record that has permanent or historic value, does not contain **Personally Identifying Information** and is not required to be retained in the office in which it was originally generated.

- An **Electronic Record** is a Record kept in an electronic format, such as a word processing document, a spreadsheet, an email, a database, a scanned or imaged document, and any other type of file stored on a computer, server, storage device or medium, or on any external or off-site storage medium, or with a third party acting as the University's agent. Electronic Records have the same retention periods as paper and other tangible Records.
- An **Inactive Record** is a Record that is no longer an Active Record but still must be maintained pursuant to the Records Retention Schedule. Inactive Records are typically maintained at an off-site storage facility or at other locations on campus.
- **Personnel** means all SJSU Staff and Faculty, full-time and part-time, including student employees acting within their scope of employment, non-employee consultants and volunteers, including Auxiliary employees.
- **Scope of Employment** means all activities related to: (i) the field or discipline of the faculty member's appointment, including the general obligation of a faculty member to teach, to do creative work, and to conduct research; and (ii) to the employment responsibilities of non-faculty personnel for which such personnel receive compensation from SJSU, where compensation is any consideration, monetary or otherwise, including the ability to use SJSU resources.
- **Confidential Record** means a record that contains confidential Level 1 or Level 2 information protected from disclosure by law or SJSU policy, including but not limited to, the Family Educational Rights and Privacy Act ("FERPA"), the Gramm Leach Bliley Act, the Health Insurance Portability Accountability Act ("HIPAA"), the California Disposal of Records Act, the California Information Security Breach and Notification Act and the SJSU Privacy Policy. See [ICSUAM8065S02 Information Security Data Classification](#).
- **Student Employee** means students, who are also SJSU employees, including Instructional Assistants.

Retention of Records

[The CSU Records Retention and Disposal Schedules](#) list different types of Records and the length of time those Records must be retained. Since no document list can cover all situations, questions regarding the retention period for a specific document or class of documents not included in the [CSU Records Retention and Disposal Schedules](#) should be addressed to the appropriate Data Steward.

Cautions Regarding Disposal

There may be conditions under which records destruction must be deferred even if they have reached or exceeded the end of their retention period. Some of these conditions include:

- All Records pertaining to ongoing or pending audits or lawsuits (including reasonably anticipated lawsuits) should not be destroyed, damaged, or altered, even if the records retention date has expired, until the matter has been resolved and you have been specifically advised in writing by campus authorities that such records may be destroyed. If you have reason to believe that a record scheduled for destruction may pertain to any of these matters, do not destroy the record and contact the Director of Internal Control.
- Records that have been requested pursuant to statute or legal proceeding (e.g., California Public Records Act, Information Practices act, or discovery of evidence in a legal proceeding) must not be disposed of while the matter is ongoing.
- External requirements under state and federal laws or regulation and University grants or contracts override university retention periods, where applicable.

- Records that have not yet been requested, but are deemed likely to be requested pursuant to stature or legal proceedings, including potential litigation, must not be disposed of until notification by the campus Risk Manager.
- Records related to any ongoing investigation must not be disposed of without prior consultation with campus counsel.

Disposal of Records

If the record retention period has expired and the record is not appropriate for the University archives, the record shall be disposed of in accordance with the [SJSU Data Disposition Standard](#).

Many of the records that the University maintains do not contain Personally Identifying Information or confidential Level 1 or Level 2 Data. Disposal of Level 3 records without Personally Identifying Information may be made by any appropriate means, including recycling of paper records.

Storing or disposing of records that contain Personally Identifying Information and/or confidential Level 1 or Level 2 Data requires special consideration. California's Disposal of Personal records Law requires the University to take appropriate measures when disposing of Personal Information, such as (a) secure shredding the record; (b) destroying the personal identifying information contained in the record; (c) modifying the record to make the personal identifying information unreadable; or (d) taking reasonable actions consistent with commonly accepted industry practice. Please refer to the [SJSU Data Disposition Standard](#).

Records Management Procedures: Annual reviews

- a) An annual inventory of all electronic and physical repositories shall be completed by each department storing data.
 - i) Annual aggregation of department inventories and review shall be completed by the Information Security Office and IDMC.
 - ii) Every mid-October, the IDMC Chair shall send out a reminder to data stewards including:
 - (1) Record custodians need to complete the review of their repositories of records.
 - (a) the annual cycle starts November 1st, and ends January 30th.
 - (b) by end of January, department MPP's must:
 - Make sure department staff are aware of the annual cycle
 - Make sure that their staff is familiar with CSU's online Schedule of Retention/Disposition.
 - Make sure that the review is carried out and all documents identified as non-retainable in accordance with the CSU Record Retention Schedule are disposed of in accordance with the SJSU Electronic Data and Disposition Standard.
 - Submit any request for exception to the Disposition rule to the Information Security Office.
 - iii) Every June, the IDMC Chair will prepare a status report of the annual review to the University President, CFO, Provost and CIO.

Definitions

CSU Records Retention Schedule: A CSU document that lists and governs the retention period of identified records that are common across the CSU. The CSU Records Retention and Disposition Schedules are published online and are accessible to any university employee with

record-keeping responsibilities. Current schedules can be found at the CSU [Records/Information Retention and Disposition website](#).

Data Steward: The individual with responsibility for the maintenance and disposition of official/original copies of records maintained by his/her department/area.

Disposition: Those associated processes associated with implementing records/information retention, destruction, or transfer decisions.

Personally identifiable information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII this includes:

- Student name, name of student's parent, or other family members; campus or home address.
- A personal identifier (such as a Social Security Number).
- A list of personal characteristics or other information which would make the student's identity easily traceable.

Record: Any information or data in any form of communication or presentation, including letters, words, pictures, sounds, or symbols, or any combination of these or other means to engage in business, regardless of media.

Appendix A – University Data Stewards and Delegates

Data Steward	Delegate	Area Represented
Beth Pugliese – <i>AVP Human Resources</i>	Carrie Medders	Human Resources
Marian Sofish - <i>SJSU Registrar</i>	Dora Ozawa	Student Records
Josee LaRochelle – CFO	Gail Finney	Finance
Meg Deiss – <i>SJSU Bursar</i>	Bobbie Seiler	Student Financials
Coleetta McElroy – <i>Director, Financial Aid</i>	Coleetta McElroy	Financial Aid
David Krack – <i>Director, Environmental Health and Safety</i>	David Krack	Environmental Health & Safety
James Sowerbrower – <i>Facilities Development & Operations</i>	James Sowerbrower	Facilities
Peter Decena – <i>Chief of Police</i>	James Renelle	University Police Department
Lelie Rohn - <i>AVP University Advancement</i>	Leslie Rohn	University Advancement
Sharon Willey – <i>AVP Admin & Enrollment Services</i>	Deanna Gonzales	Admissions
Elna Green - <i>AVP Faculty Affairs</i>	Elna Green	Faculty Affairs
Stacy Gleixner – <i>AVP Student Academic Success Services</i>	Stacy Gleixner	Curriculum & Accreditation
Pamela Stacks – <i>AVP Research</i>	Pamela Stacks	Research & Sponsored Programs
Marna Genes – <i>AVP Academic Budgets & Planning</i>	Scott Heil	Institutional Records