

Policy 118

**Records/Information Retention and
Disposition Policy**

Section: 100 – General Administration
Responsible Executive: Lead Financial
Administrator
Responsible Department: Business and Finance
Office
First Effective Date: October 29, 2010
Last Reviewed: March 2018
Next Scheduled Review: June 2020

1.0 PURPOSE

- 1.1. To provide for orderly and proper retention and destruction of all official records.

2.0 BACKGROUND

- 2.1. The Cal Poly Corporation (CPC) is committed to effective records management to meet legal standards, ensure privacy, optimize the use of space, destroy outdated records in an appropriate manner, improve operational efficiency and effectiveness, and comply with California State University (CSU) policy and all applicable laws and regulations. CSU Executive Order 1031, “System wide Records/Information Retention and Disposition Schedules Implementation,” requires that legal and regulatory requirements associated with the retention and disposition of CSU records/information are met.

3.0 POLICY

- 3.1. Standards and Schedules. The retention and disposition of records/information are to conform to standards and schedules set forth within retention and disposition schedules issued by the CSU and this policy. In addition, CPC’s policy must ensure that the designation of a vital Record/Information is consistent with CPC’s business continuity plan.
- 3.2. Confidentiality Requirement. Records containing confidential and personal data will be accessed only by authorized persons, maintained in secured and/or locked locations, and destroyed by appropriate methods. Refer to the CPC’s Information Security Awareness Policy for more specific information.
- 3.2.1. All employees who handle confidential data will complete the University’s Web-based Information Security Awareness Program or a similar program when hired and then updated as required by the University.
- 3.3. Department or Unit Responsibilities.
- 3.3.1. For departments or units that maintain CPC records, within that department or unit, each Records/Information Custodian is responsible for:
- 3.3.1.1. Implementing the records management practices consistent with this policy;
 - 3.3.1.2. Educating staff in understanding sound record management practices;
 - 3.3.1.3. Ensuring that access to confidential records and information is restricted;
 - 3.3.1.4. Ensuring destruction of inactive records that have no value upon passage of the applicable retention period;
 - 3.3.1.5. Ensuring that records are destroyed in a manner that is appropriate for the type or records and information involved;
 - 3.3.1.6. Providing CPC Records Retention Designee with updates of the master log of items stored at the Warehouse and off-site; and
 - 3.3.1.7. Preparing records for storage including labeling boxes and moving files.

3.4. Electronic Records.

- 3.4.1. Electronic records and files should be treated with the same confidentiality and security as hard copy documents.
- 3.4.2. Computer users are responsible for the maintenance and security of their electronic files and data.
- 3.4.3. The Information Technology department (“IT”), or Cal Poly Information Services (as appropriate based on location and oversight of equipment), are responsible for backing up the servers.
- 3.4.4. Computer records should be retained according to the same retention periods as paper records.
- 3.4.5. Users should review and delete any unused or obsolete files on a regular basis, but no less than annually, unless litigation or other restrictions are in effect.
- 3.4.6. Users should periodically log on to the network to clean up their email accounts.
- 3.4.7. Computer users will adhere to all University and CPC IT procedures and guidelines.

3.5. Record Storage Protocol.

- 3.5.1. Records stored in boxes and/or warehoused outside of the CPC Business office must be stored as follows:
 - 3.5.1.1. Storage boxes must be medium or heavy duty banker’s boxes (i.e. preferably #707 or #737 for authorization and check copies, and #701 for cancelled checks)
 - 3.5.1.2. Permanent records should be stored in dark brown banker’s boxes (i.e. #725) when at all feasible to be easily distinguished from non-permanent records.
 - 3.5.1.3. Permanent records should be stored on a separate pallet in the Warehouse.
- 3.5.2. Storage boxes must be labeled with the following information easily visible on both ends:
 - 3.5.2.1. Company,
 - 3.5.2.2. Document number range (From-To),
 - 3.5.2.3. Date range,
 - 3.5.2.4. Description (i.e. check copies, voucher checks, authorizations); and
 - 3.5.2.5. Destroy date or so noted if permanent retention.
- 3.5.3. Storage boxes should generally be stacked no more than three (3) rows high on a pallet, with safety and maintaining the integrity of the storage containers the primary concern.
- 3.5.4. A master log of boxes and pallets stored off-site will be maintained by the CPC Records Retention Designee and each department utilizing the off-site storage is responsible for providing updates to the master log.
- 3.5.5. The off-site storage log should be reviewed annually for scheduling of record destruction as needed.

3.6. Disposal and Destruction of Records.

- 3.6.1. Upon determination that it is appropriate to dispose of certain records, they should be destroyed in one of the following ways:
 - 3.6.1.1. Recycled non-confidential paper records;
 - 3.6.1.2. Shred or otherwise render unreadable confidential paper records; or
 - 3.6.1.3. Erase or destroy electronically stored data.

3.7. Retention Periods.

3.7.1. General categories of records subject to specific retention periods are described in Record and Retention Procedures, which lists financial and other documents and their recommended retention periods. This document is not to be considered an all-inclusive listing for retention purposes, but describes the more frequent or commonly used records that need to be retained. If specific records are not listed, it does not mean that they can or should be discarded or destroyed without first considering the general requirements in this policy.

3.7.2. Retention periods may increase by government regulation, judicial or administrative order, private or governmental contract, pending litigation or audit requirements.

4.0 DEFINITIONS

4.1. Records/Information Custodians. Each unit or department will designate a person as the department's "Records/Information Custodian" who will be responsible for the control and administration of records/information in all media forms and for valuing such records/information in accordance with this policy.

4.2. CPC Records Retention Designee. An individual will be identified by the Executive Director or his/her designee to be responsible for the overall record-keeping of CPC.

4.3. Off-site. Items which are stored at a third-party vendor's location.

4.4. Record/Information. Every means of recording upon any tangible thing in any form of communication or representation, including letters, words, pictures, sounds, or symbols, any combination of these or other means to engage in business, regardless of media. This includes, but is not limited to:

4.4.1. Electronic communication such as e-mail content and attachments, voicemail, instant messages, and data on a contactless integrated circuit;

4.4.2. Content on web sites, PDA's, mobile devices, desktops, and servers;

4.4.3. Information/data captured in various databases;

4.4.4. Physical paper in files, such as memos, contacts, reports, photographs and architectural drawings;

4.4.5. Licenses, certificates, registration, identification cards, or other means;

4.4.6. Handwriting, typewriting, printing, Photostatting, photographing, photocopying, transmitting by electronic email or facsimile;

4.4.7. Any record thereby created, regardless of the manner or media in which the record has been stored and/or created; and

4.4.8. Backups of electronic information.

5.0 PROCEDURES, GUIDELINES AND FORMS

5.1. The Lead Financial Administrator, or his/her designee, is charged with the responsibility of implementing this policy through procedures, guidelines and forms, if needed. This includes the responsibility and right to set or modify the retention schedule of any CPC records, while still complying with applicable law and CSU policy.

5.2. The following guidelines currently exist:

5.2.1. CPC Records and Retention Procedures

5.2.2. CPC Information and Security Guidelines

5.2.3. CPC Software and Hardware Guidelines

5.2.4. CPC Remote Access Guidelines

5.2.5. CPC Litigation Hold Guidelines

5.2.6. CPC's Plan for Safeguarding Confidential Information (per §3.2 above).

6.0 COMPLIANCE

6.1. All CPC units, departments and personnel must comply with this policy.

7.0 REFERENCES AND RELATED POLICY

7.1. CSU Executive Order 1031 System wide Records/Information Retention and Disposition Schedules Implementation, February 27, 2008

7.2. Current retention schedules can be found at the CSU Records/Information Retention and Disposition website, <http://www.calstate.edu/recordsretention/>

Technical and administrative change updates

9-12-12 for title and organization structure changes.