



OFFICE OF THE EXECUTIVE VICE PRESIDENT—
CHIEF FINANCIAL OFFICER

OFFICE OF THE PRESIDENT
1111 Franklin Street, 6th Floor
Oakland, California 94607-5200

August 21, 2018

CHANCELLORS
ACADEMIC COUNCIL CHAIR MAY
LABORATORY DIRECTOR WITHERELL
ANR VICE PRESIDENT HUMISTON

Re: Systemwide Review of Proposed Presidential Policy “Principles of Accountability with Respect to Financial Transactions”

Dear Colleagues:

Attached for Systemwide Review is a new Presidential Policy, Principles of Accountability with Respect to Financial Transactions. The main impetus is to codify an existing UCOP Financial Policy currently posted on the Chief Financial Officer website into the presidential policy template. In 2016, the draft policy was distributed to key stakeholder groups: Campus Controllers and their constituents. The working group that reviewed the draft provided comments related to the existing UCOP Financial Policy. The draft was revised to address the principles of financial stewardship. The revised document follows the 2013 Committee on Sponsoring Organizations of the Treadway Commission (“COSO”) Internal Control-Integrated Framework. All of the comments received were incorporated into the new policy that is submitted for systemwide review.

Systemwide Review

Systemwide review is a public review distributed to the Chancellors, the Director, Lawrence Berkeley National Laboratory, the Chair of the Academic Council, and the Vice President of Agriculture and Natural Resources requesting that they inform the general University community, affected employees, and union membership about policy proposals. Systemwide Review also includes a mandatory, three-month full Senate review. Employees should be afforded the opportunity to review and comment on the draft policy.

Attached is a Model Communication which may be used to inform non-exclusively represented employees about this proposal. The Labor Relations Office at the Office of the President is responsible for informing the bargaining units representing union membership about policy proposals.

We would appreciate receiving your comments no later than December 17, 2018. Please submit all comments to ruth.satorre@ucop.edu. If you have questions, please contact Ruth Satorre at (510) 987-0414.

Systemwide Review
August 21, 2018

Sincerely,



Peggy Arrivas
AVP- Systemwide Controller

cc: President Napolitano
Provost and Executive Vice President Brown
Executive Vice Chancellors/Provosts
President's Advisory Group
Vice President Duckett
Vice President Ellis
Vice President Holmes-Sullivan
Vice Provost Carlson
Vice Provost Gullatt
Deputy General Counsel Woodall
Vice Chancellors/Vice Provosts of Academic Personnel/Academic Affairs
Academic Personnel Directors
Chief of Staff Nava
Deputy Compliance Officer Myjer
Executive Director Baxter
Executive Director Peterson
Executive Director Chester
Director Hairston
Director Grant
Manager Smith
Manager Steinhoff
Manager Jordan
Manager Crosson



OFFICE OF THE VICE PRESIDENT AND
CHIEF INFORMATION OFFICER
Information Technology Services

OFFICE OF THE PRESIDENT
1111 Franklin Street, 7th Floor
Oakland, California 94607-5200

September 17, 2018

CHANCELLORS
ACADEMIC COUNCIL CHAIR MAY
LABORATORY DIRECTOR WITHERELL
ANR VICE PRESIDENT HUMISTON

Re: Systemwide Review of Proposed Presidential Policy BFB-RMP-7 Protection of Administrative Records Containing Personally Identifiable Information

Dear Colleagues:

Attached for Systemwide Review is a proposed revision of Presidential Policy BFB-RMP-7, Protection of Administrative Records Containing Personally Identifiable Information.

The University of California Records Management Committee (RMC) is reviewing and updating policies in the BFB-RMP series. As a result of that review, it is consolidating and updating three policies in the series that cover related topics – BFB-RMP-7, Privacy of and Access to Information Responsibilities; BFB-RMP-11, Student Applicant Records; and BFB-RMP-12, Guidelines for Assuring Privacy of Personal Information in Mailing Lists and Telephone Directories. These policies are found at <https://www.ucop.edu/information-technology-services/policies/records-management-policies.html>. Also attached is a redline document that compares language in existing policies RMP-7, RMP-11, and RMP-12 with the proposed revision of RMP-7.

The scope of the revised policy is limited to personally identifiable information in administrative records, regardless of whether the records are in paper, electronic, or other media. BFB-RMP-1, University Records Management Program, defines administrative records as follows:

“The term ‘**administrative record**’ is used to describe any record that documents or contains valuable information related to the organization, functions, policies, decisions, procedures, operations, or other business activities of the university.”

BFB-RMP-1 also states that the Records Management Program:

“...applies to all administrative records, regardless of their medium. The Program does not apply to:

- Administrative records held by the Principal Officers of The Regents,
- Teaching and research records (e.g., library materials, faculty research and teaching materials, student examinations), or
- Records pertaining to individual patient care (medical records).”

September 17, 2018

Page 2

In consolidating the three existing policies into a revised and updated RMP-7, the RMC eliminated sections that are no longer pertinent, retained sections that are still relevant, and updated others. The revised policy clarifies the roles of Privacy Officials, Records Management Coordinators, and Information Practices Coordinators, and incorporates the UC Statement of Privacy Principles and Values.

UC Records Manager Laurie Sletten, former Systemwide Privacy Manager Roslyn Martorano, and, recently, current Systemwide Privacy Compliance Manager Scott Seaborn led the review and developed the draft in conjunction with a committee of Records Management Coordinators and Privacy Officers. The draft has undergone significant systemwide review and been revised to reflect input from key functional areas. The draft was first presented to the Policy Advisory Committee (PAC) in September 2016, after which it was vetted with various groups, as shown below:

- Records Management Coordinators: 11/28/2016, 1/17/2017, 1/26/2017, 6/15/2017, 1/22/2018
- Information Practices Coordinators: 11/28/2016, 6/15/2017
- Privacy Officers: 11/28/2016, 1/17/2017, 6/15/2017, 7/26/2018
- HIPAA Officers: 11/28/2016, 1/17/2017, 6/15/2017
- Office of the General Counsel: 1/17/2017, 6/15/2017, 7/26/2018
- Information Security: 11/28/2016, 1/17/2017, 1/26/2017

The updated draft was re-presented to the PAC on June 20, 2018, at which point the PAC recommended initiation of the formal Systemwide Review.

Systemwide Review

Systemwide Review is a public review distributed to the Chancellors, the Director, Lawrence Berkeley National Laboratory, the Chair of the Academic Council, and the Vice President of Agriculture and Natural Resources requesting that they inform the general University community, affected employees, and union membership about policy proposals. Systemwide Review also includes a mandatory, three-month full Senate review. Employees should be afforded the opportunity to review and comment on the draft policy. Attached is a Model Communication which may be used to inform non-exclusively represented employees about these proposals. The Labor Relations Office at the Office of the President is responsible for informing the bargaining units representing union membership about policy proposals.

If you have any questions, please contact UC Records Manager Laurie Sletten at 510-987-9411. Please submit your comments to Laurie Sletten at laurie.sletten@ucop.edu no later than December 17, 2018.

Sincerely,



Tom Andriola
Vice President & UC Chief Information Officer
Information Technology Services

September 17, 2018

Page 3

Attachments: Proposed Presidential Policy BFB-RMP-7, Protection of Administrative Records
Containing Personally Identifiable Information
Redline of Existing RMP-7, RMP-11, and RMP-12
Model Communication

cc: President Napolitano
Provost and Executive Vice President Brown
Executive Vice Chancellors/Provosts
President's Advisory Group
Vice President Duckett
Vice President Ellis
Vice President Holmes-Sullivan
Vice Provost Carlson
Vice Provost Gullatt
Deputy General Counsel Woodall
Vice Chancellors/Vice Provosts of Academic Personnel/Academic Affairs
Academic Personnel Directors
Chief of Staff Nava
Deputy Compliance Officer Myjer
Executive Director Baxter
Executive Director Peterson
Executive Director Chester
Director Hairston
Director Grant
Manager Smith
Manager Steinhoff
Manager Jordan
Manager Crosson



BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

Responsible Officer:	Chief Information Officer & Vice President – Information Technology Services
Responsible Office:	ITS – Information Technology Services
Issuance Date:	
Effective Date:	
Last Review Date:	
Scope:	This applies to all University employees, students and others who have authorized access to Administrative Records containing Personally Identifiable Information at all locations.

Contact:	Laurie Sletten
Title:	UC Records Manager
Email:	laurie.sletten@ucop.edu
Phone #:	(510) 987-9411

TABLE OF CONTENTS

I. POLICY SUMMARY	2
II. DEFINITIONS.....	2
III. POLICY TEXT	5
IV. COMPLIANCE / RESPONSIBILITIES.....	8
V. PROCEDURES	10
VI. RELATED INFORMATION	12
VII. FREQUENTLY ASKED QUESTIONS	13
VIII. REVISION HISTORY	13

I. POLICY SUMMARY

The University of California respects the privacy of individuals as fundamental to its mission and a value enshrined in the California constitution. Privacy:

1. Is essential to promoting the values of academic and intellectual freedom,
2. Plays an important role in upholding human dignity and safeguarding a strong, vibrant society, and
3. Serves as the basis for an ethical and respectful workplace.

The University is committed to protecting personal privacy in its operations, activities, and management of information. The University must balance this commitment with other important commitments, including public accountability and the right of people to access information about the conduct of the public's business. This policy outlines the requirements and processes for ensuring the University protects information by meeting its legal obligations, as well as balancing information privacy and autonomy privacy with competing institutional obligations, values, and interests.

The purpose of this bulletin is to establish the systemwide processes for safeguarding personally identifiable information in Administrative Records. When personally identifiable information is requested, the University must examine whether its disclosure or use is governed by law or University policy, and if not, whether disclosure or use constitutes an unwarranted invasion of personal privacy. If the University's response to the request is not mandated by law or policy, the requested personally identifiable information may be released, used or disclosed only after a balancing analysis determines that it does not constitute an unwarranted invasion of personal privacy.

This policy is for use by anyone in the University community who makes decisions about Administrative Records. Material provided in the procedures may be helpful to anyone in the institution who creates or receives records of any type.

II. DEFINITIONS

Administrative Records: As defined in [Business and Finance Bulletin Records Management and Privacy-1: University Records Management Program](#) (RMP-1), this term is used to describe any record, regardless of physical form or characteristics, that documents or contains valuable information related to the organization, functions,

BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

policies, decisions, procedures, operations, or other business activities of the University.¹

California Information Practices Act (IPA): The law that guarantees the right of access to records containing an individual’s personal information, with certain limitations, and sets forth provisions to govern the collection, maintenance, accuracy, dissemination, and disclosure of information about them. Special procedures for providing access to and protecting the privacy of University records containing personal data are required by the IPA.

California Public Records Act (CPRA): The law that provides public access to state and local agency records relating to the conduct of the public’s business. Public records must be disclosed upon request, unless a statutory exemption applies. In providing access, CPRA remains mindful of individual privacy rights.

Campus Privacy Official: The individual at each location responsible for overseeing the strategic direction and application of the [UC Statement of Privacy Values & Privacy Principles](#)² and UC Privacy Balancing Process.

Commercial Purposes: Any purpose that has financial gain as a major objective.

Family Educational Rights and Privacy Act (FERPA): The federal law that addresses the privacy of students’ educational records, which are records directly related to a student and are maintained by the University or a party acting for or on behalf of the University.

General Data Protection Regulation (“GDPR”): A privacy law of the European Union that governs the use of personally identifiable information. It concerns the personal data of individuals in the European Economic Area (EEA), which includes EU countries as well as the United Kingdom, Iceland, Norway, and Lichtenstein. The GDPR defines "personal data" very broadly such that the term includes names, addresses, phone numbers, national IDs, IP addresses, profile pictures, personal healthcare data, educational data, and any other data that can be used to identify an individual. It addresses multiple issues, such as the rights of data subjects, consent, and purpose of use.

¹ Administrative records do not include the records held by the Principal Officers of The Regents; teaching and research records (e.g., library materials, faculty research and teaching materials, student examinations); or records pertaining to individual patient care (medical records).

² For more information, see Section IV.C. Roles and Responsibilities. A list of current privacy officials can be found at <http://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/campus-privacy-officials.html>.

BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

Information Practices Coordinator: The individual at each location responsible for administering responses to records requests, and providing guidance to constituents at their locations on matters related to the access, use, and disclosure of information maintained in Administrative Records.

Information Privacy: As defined in the [UC Statement of Privacy Values & Privacy Principles](#), is the appropriate protection, use, and dissemination of information about individuals.

Mailing Lists: Any compilation of names and addresses, including email addresses.

Personally Identifiable Information (PII): Any information that describes or identifies an individual, including but not limited to name, Social Security number, physical description, home address, telephone numbers, email address, education, financial matters, medical or employment history, or statements made by or attributed to the individual.

Privacy and Information Security Board: The privacy and information security board at each location that advises on privacy and information security; sets strategic direction for autonomy privacy, information privacy, and information security; champions the UC Privacy Values & Privacy Principles, and the UC Privacy Balancing Process; and monitors compliance and assesses risk and effectiveness of location privacy and information security programs. These boards may be separate committees or structured as part of an existing location governance committee.

Records Management Coordinator: As defined in [RMP-1](#), the individual at each location responsible for the development, coordination, implementation, and management of the Records Management Program at the location.

Records Management Program: In accordance with [RMP-1](#), the Program that promotes sound, efficient, and economical records management in the following areas: (1) creation, organization of, and access to records; (2) maintenance and retention of Administrative Records; (3) security and privacy of records; (4) protection of records vital to the University; (5) preservation of records of historical importance; (6) disposition of Administrative Records when they no longer serve their purpose; and (7) other functions the University may deem necessary for good records management.

Student Applicant Records: Records of a person during the period of application, acceptance, and admission to the University, *prior* to enrollment.

Telephone Directories: A collection of individuals' names, telephone numbers, and other contact information, including employee (campus) or student directories.

UC Privacy Balancing Process: The process designed to address privacy risks when there is no policy in place pertaining to the situation.³

III. POLICY TEXT

This policy applies to all Personally Identifiable Information (PII) in the University of California’s Administrative Records, regardless of the record’s function or medium, and addresses requirements related to the treatment of such information. Requests for academic personnel records from government agencies are governed by Business and Finance Bulletin Records Management and Privacy Policies [9a](#), [9b](#), and [9c](#).⁴

All faculty, staff, and other individuals associated with the University who have access to Administrative Records containing PII must understand their responsibilities for safeguarding the privacy of that information. The Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators in consultation with the UC Office of the General Counsel (OGC), are responsible for providing overall policy and procedural guidance to University locations about privacy of and access to Administrative Records.⁵

A. Rules of Conduct for Employees with Access to Information Concerning Individuals

The University of California requires employees to adhere to the following rules of conduct concerning minimum standards⁶ for the collection, maintenance, disclosure, safeguarding, and destruction of Administrative Records containing PII. The California Information Practices Act (IPA) requires that any officer or employee who intentionally violates this policy, including these rules of conduct, may be subject to discipline, up to and including termination.⁷

1. Employees responsible for the collection, maintenance, use, and dissemination of Administrative Records that contain PII, must comply with the provisions of the IPA.

³ See [UC Privacy and Information Security Steering Committee Report to the President January 2013](#), page 18

⁴ For additional requirements concerning requests for and access to academic peer review records, see policy APM-160.

⁵ For more information about the specific responsibilities of each role, see Section IV.C.

⁶ See [Rules of Conduct for University Employees Involved with Information Regarding Individuals](#), part of the Privacy Principles and Practices at UC

⁷ California Civil Code § 1798.55

University of California – Policy BFB-RMP-7

BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

2. Employees must not require individuals to disclose PII about themselves or others that is not necessary and relevant to the purposes of the University or to the particular function for which the employee is responsible.
3. Employees must make every reasonable effort to ensure inquiries and requests by individuals for records containing their PII are responded to quickly, courteously, and without requiring the requester to repeat the inquiry to others unnecessarily.
4. Employees must assist individuals seeking information pertaining to themselves with making their inquiries sufficiently specific and descriptive to facilitate locating the records.
5. Employees must not disclose PII to unauthorized persons or entities.
6. Employees must not seek out or use PII relating to others for their own interest or advantage.
7. Employees responsible for the maintenance of records containing PII must take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the records from unauthorized access, use and disclosure.

B. Management of Records containing PII

For specific procedures concerning mailing lists and student records including application records, see Section VI Procedures. For information concerning academic peer review records, see [APM-160](#).

The University strives to collect and maintain only information that is necessary and pertinent to accomplish its University mission.

To the greatest extent practicable, information about an individual must be collected directly from the individual to whom it pertains. When this is not possible, the University must maintain the source or sources of information, in a readily accessible format, in order to provide the source or sources to the individual upon request. When PII is disclosed, individuals may be notified according to existing legal requirements, University policy, and campus practices.

Each location must establish procedures that ensure an individual's right to inquire and be notified whether the University maintains records about them; and provide the records for inspection by the individual to the extent required by law. These procedures

must be consistent with the requirements of the IPA, and University policies, such as [UC IS-3 Electronic Information Security](#).

1. Use of PII for Commercial Purposes

The University prohibits employees responsible for maintaining or accessing records with PII from distributing, selling, or renting PII for commercial purposes unless such action is specifically authorized by law.⁸

2. Disposition of Administrative Records Containing PII

Information held by the University must be disposed of in accordance with federal and state law, and as required by [RMP-2 Records Retention and Disposition](#) and the [UC Records Retention Schedule](#), unless it is needed as evidence in an investigation, foreseeable or on-going litigation, on-going audit, on-going records request or other special circumstance – in which case the information must be retained until these actions have been completed or resolved.

3. Procedures for Reporting Unauthorized Disclosures or Breaches of PII

Each location is responsible for developing its procedures for reporting unauthorized disclosures or breaches of PII for both paper and electronic records. Procedures for reporting electronic unauthorized disclosures or breaches of PII must be consistent with the University of California Privacy and Data Security Incident Response Plan.

4. General Data Protection Regulation (“GDPR”) Requirements

GDPR requirements may be more restrictive and UC guidance for it must be consulted.

C. Evaluating Use or Disclosure of PII

When neither law nor policy provides definitive guidance regarding a proposed use or disclosure of PII, the University must use the [UC Privacy Balancing Process](#) to adjudicate privacy and other competing interests.

Under the Balancing Process, the University must not make public disclosures of information when it can demonstrate that the public interest served by nondisclosure clearly outweighs the public interest served by disclosing the information. In reaching this decision, the University must review specific statutory exceptions that might allow

⁸ For example California Civil Code §1798.60

for disclosure of PII. Situations involving unprecedented and significant balancing concerns are referred to the location's Privacy Board unless a relevant alternative adjudication path is already established.

IV.COMPLIANCE / RESPONSIBILITIES

A. Implementation of the Policy

The Vice President for Information Technology Services and Chief Information Officer is responsible for issuing and updating any requirements, standards or guidelines that support this policy.

Chancellors, the Vice President of Agriculture and Natural Resources, and UC Managed Laboratory Directors are responsible for designating an Information Practices Coordinator, Campus Privacy Official, and Records Management Coordinator to administer and implement this policy at their location.

The UC Information Practices Coordinator, UC Privacy Manager, and UC Records Manager facilitate regular communication among local Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators to address consistent implementation of this policy throughout the University. Each Information Practices Coordinator, Privacy Official, and Records Management Coordinator must work together at their locations to ensure consistent implementation of this policy, as necessary.

B. Revisions to the Policy

The Vice President for Information Technology Services and Chief Information Officer has the authority to initiate policy revisions and is responsible for regular reviews and updates consistent with approval authorities and applicable Bylaws and Standing Orders of The Regents.

C. Roles & Responsibilities

The following functions are critical to ensuring the University handles information in a manner consistent with the University's legal obligations, policy requirements, and the [UC Statement of Privacy Values & Privacy Principles](#). Together, Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators serve

BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

as subject matter experts and collaborate with other disciplines to strengthen the University's information governance framework.

1. University Employees

All faculty, staff, and other University community members with access to records with PII must safeguard the records from unauthorized access, use and disclosure.

2. University Managers

All managers must ensure that any personnel who have access to records with PII are made aware of their responsibilities for handling such records, including protecting the records from unauthorized access, use and disclosure.

3. Information Practices Coordinators

The Information Practices Coordinator at each location is responsible for administering responses to records requests, and providing guidance on matters related to the access, use, and disclosure of information maintained in Administrative Records. The California Public Records Act (CPRA) Office within the OGC provides guidance to campuses and may manage multi-campus CPRA requests on behalf of the locations. At their locations, Information Practices Coordinators also:

- i. Ensure that procedures and practices for access, amendment, use and disclosure of Administrative Records adhere to federal and state laws, including but not limited to the IPA and the CPRA.
- ii. Develop guidelines, including training programs, on IPA and CPRA practices, including the rules of conduct outlined in Section III.A.
- iii. Review local PII collection and notice practices upon request.
- iv. Assist with interpretation of federal and state privacy and disclosure laws and University policies including but not limited to the CPRA, IPA and the UC rules of conduct outlined in Section III.A.

4. Campus Privacy Officials

Campus Privacy Officials at each location are responsible for overseeing the strategic direction and application of the [UC Statement of Privacy Values & Privacy Principles](#), and UC Privacy Balancing Process throughout the activities at that location.

5. Records Management Coordinators

As defined in [RMP-1](#), Records Management Coordinators are responsible for the development, coordination, implementation, and management of the Records Management Program at their locations.

6. Chancellors, the Vice President of Agriculture and Natural Resources, and UC Managed Laboratory Directors

These positions are responsible for designating an Information Practices Coordinator, Campus Privacy Official, and Records Management Coordinator to administer and implement this policy at their locations.

7. The Vice President for Information Technology Services and Chief Information Officer

This position is responsible for issuing and updating any requirements, standards or guidelines that support this policy.

V. PROCEDURES

For specific categories of PII, all locations must follow the procedures below to ensure consistency across the University.

A. Student Applicant Records

In accordance with California law, the University only collects information relevant to the University's purposes. Disclosure of this information must be in accordance with state and federal law.

Until an applicant has enrolled in an academic program, any records referring to them are considered student applicant records and must be used and accessed in a manner consistent with the protections afforded by the IPA.

Records directly related to an enrolled student, including the student's applicant records, are subject to the Family Educational Rights and Privacy Act (FERPA).⁹

⁹ For policy requirements and further information about privacy and potential disclosure of student records, please read [Policies Applying to the Disclosure of Information from Student Records](#) (UC PACAOS-130)

BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

An applicant has the right to inspect records that reference them in relation to the application process, and are maintained in the applicant's file, with the exception of recommendation letters and associated records created with the documented understanding of confidentiality.¹⁰

When the applicant is outside the United States, they may have a person within the U.S. act as their representative. This representative has the same right of access to the applicant's file. The University may disclose information to this representative if records within the University's possession demonstrate with reasonable certainty that this is the applicant's intended representative.

1. Parents of Applicants

In accordance with the IPA, the University must not release information from the applicant's records to the applicant's parents without the applicant's written consent, regardless of the individual's age or financial status. The University's current admissions process provides the opportunity to furnish this consent.

In accordance with FERPA, the University must not release student records (including application records) to parents without the student's written consent, regardless of age or financial status, unless such release falls under a specific exception under FERPA.

2. Third Parties

In accordance with state law, the University may disclose PII about a University applicant to certain third parties (e.g., high school counselors). This information may include eligibility status or lack of certain grades. The University may disclose this information only if:

- a. The applicant gives prior written consent;
- b. The information is necessary for performance of the third party's official duties and its use is compatible with its original collection purpose;
- c. The requested information will be used for scientific or statistical research and assurances of confidentiality and protection of personal identity are guaranteed; or
- d. Other legal exceptions apply.

3. Advancement, Development, and Alumni Office Staff

¹⁰ California Civil Code §1798.38; 20 USC § 1232g(a)(1)(C)

Advancement, Development, and Alumni office staff have legitimate educational interest in applicants' records. These offices may access applicant information, including PII, when the information is relevant and necessary to carry out their assigned duties and is clearly related to the purpose for which the information was originally collected.

B. University Mailing Lists and Telephone Directories

Upon written request from any individual, any University office that maintains a Mailing List must remove that individual's name and address from such list, unless the list is used by the University solely for necessary direct contact with the individual.

The University must not use or disclose its Telephone Directories and Mailing Lists for commercial purposes, unless such action is specifically authorized by law.

VI. RELATED INFORMATION

Academic Personnel Manual

- [Section 160](#), Maintenance of, Access to, and Opportunity to Request Amendment of Academic Personnel Records

Business and Finance Bulletins

- [IS-3](#), Electronic Information Security
- [RMP-1](#), University Records Management Program
- [RMP-2](#), Records Retention and Disposition
- [RMP-9a](#), [-9b](#), [-9c](#), Guidelines for Access to University Personnel Records by Governmental Agencies

Personnel Policies for Staff Members

- [PPSM 21](#), Selection and Appointment

Federal and State Laws

- California Constitution, Article I, Section 1 and 3
- California Information Practices Act
- California Public Records Act
- Family Educational Rights and Privacy Act

Other Presidential Policies and Guidelines

- [Electronic Communications Policy](#)
- [Gramm-Leach-Bliley Compliance Plan](#)
- [UC Policy on Public Disclosure of Compensation Information](#)
- [UC Privacy Balancing Process](#)
- [UC Privacy and Data Security Incident Response Plan](#)
- [UC Privacy and Information Security Steering Committee Report to the President January 2013](#)
- [UC Statement of Privacy Values & Privacy Principles](#)

Other

- [UC Procurement Appendix DS — Data Security and Privacy](#)

For specific additional requirements about Student Records, Protected Health Information (PHI), and Academic Peer Review Records please refer to the policies below:

- Student Education Records: UC PACAOS-130 [Policies Applying to the Disclosure of Information from Student Records](#) and the Federal Family Educational Rights and Privacy Act (FERPA) primarily govern the handling of student education records.
- Protected Health Information: The [University's HIPAA policies](#), the Health Information Portability and Accountability Act of 1996 (HIPAA), and subsequent amendments in the Health Information Technology for Economic and Clinical Health (HITECH) Act govern the handling of Protected Health Information.
- Academic Peer Review Records: See [APM 160-20](#)
This policy defines the rights of individuals and entities to have access to academic peer review records.

VII. FREQUENTLY ASKED QUESTIONS

Not applicable

VIII. REVISION HISTORY

Revision Date: This Policy was remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

University of California – Policy BFB-RMP-7

BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

This policy replaces the following policies:

- BFB-RMP-7: Privacy of and Access to Information Responsibilities. November 1, 1985 Initial Version.
- BFB-RMP-8: Requirements of Privacy of and Access to Information. November 13, 2015 Rescinded.
- BFB-RMP-11: Student Applicant Records. June 15, 1989 Initial Version.
- BFB-RMP-12: Guidelines for Assuring Privacy of Personal Information in Mailing Lists and Telephone Directories. June 15, 1989 Initial Version

BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

NUMBER RMP:

Formatted: Highlight

PRIVACY OF AND ACCESS TO INFORMATION RESPONSIBILITIES

REFER ALL SYSTEMWIDE QUESTIONS TO:

Coordinator of Information Practices

REFER ALL CAMPUS QUESTIONS TO:

Information Practices Coordinator

EFFECTIVE DATE:

November 1, 1985

I. REFERENCE

Business and Finance Bulletin RMP-8, "Privacy of and Access to Information, Legal Requirements," November 1, 1985.

<u>Responsible Officer:</u>	<u>Chief Information Officer & Vice President – Information Technology Services</u>
<u>Responsible Office:</u>	<u>ITS – Information Technology Services</u>
<u>Issuance Date:</u>	
<u>Effective Date:</u>	
<u>Last Review Date:</u>	
<u>Scope:</u>	<u>This applies to all University employees, students and others who have authorized access to Administrative Records containing Personally Identifiable Information at all locations.</u>

<u>Contact:</u>	<u>Laurie Sletten</u>
<u>Title:</u>	<u>UC Records Manager</u>
<u>Email:</u>	<u>laurie.sletten@ucop.edu</u>
<u>Phone #:</u>	<u>(510) 987-9411</u>

TABLE OF CONTENTS

I. POLICY SUMMARY	ERROR! BOOKMARK NOT DEFINED.
II. DEFINITIONS	3
III. POLICY TEXT	6
IV. COMPLIANCE / RESPONSIBILITIES.....	9
V. PROCEDURES.....	ERROR! BOOKMARK NOT DEFINED.
VI. RELATED INFORMATION	21
VII. FREQUENTLY ASKED QUESTIONS	23
VIII. REVISION HISTORY	23

II. SCOPE

This Bulletin establishes responsibilities for privacy of and access to all information maintained by any segment of the University, except for those records pertaining to students. (See "Policies Applying to Campus Activities, Organizations, and Students—Part B, University of California Policies Applying to the Disclosure of Information from Student Records, October 31, 1983.")

I. POLICY SUMMARY

The University of California respects the privacy of individuals as fundamental to its mission and a value enshrined in the California constitution. Privacy:

1. Is essential to promoting the values of academic and intellectual freedom,
2. Plays an important role in upholding human dignity and safeguarding a strong, vibrant society, and
3. Serves as the basis for an ethical and respectful workplace.

The University is committed to protecting personal privacy in its operations, activities, and management of information. The University must balance this commitment with other important commitments, including public accountability and the right of people to access information about the conduct of the public's business. This policy outlines the requirements and processes for ensuring the University protects information by meeting its legal obligations, as well as balancing information privacy and autonomy privacy with competing institutional obligations, values, and interests.

The purpose of this bulletin is to establish the systemwide processes for safeguarding personally identifiable information in Administrative Records. When personally identifiable information is requested, the University must examine whether its disclosure or use is governed by law or University policy, and if not, whether disclosure or use constitutes an unwarranted invasion of personal privacy. If the University's response to the request is not mandated by law or policy, the requested personally identifiable information may be released, used or disclosed only after a balancing analysis determines that it does not constitute an unwarranted invasion of personal privacy.

This policy is for use by anyone in the University community who makes decisions about Administrative Records. Material provided in the procedures may be helpful to anyone in the institution who creates or receives records of any type.

II. DEFINITIONS

Administrative Records: As defined in Business and Finance Bulletin Records Management and Privacy-1: University Records Management Program (RMP-1), this term is used to describe any record, regardless of physical form or characteristics, that documents or contains valuable

information related to the organization, functions, policies, decisions, procedures, operations, or other business activities of the University.¹

California Information Practices Act (IPA): The law that guarantees the right of access to records containing an individual's personal information, with certain limitations, and sets forth provisions to govern the collection, maintenance, accuracy, dissemination, and disclosure of information about them. Special procedures for providing access to and protecting the privacy of University records containing personal data are required by the IPA.

California Public Records Act (CPRA): The law that provides public access to state and local agency records relating to the conduct of the public's business. Public records must be disclosed upon request, unless a statutory exemption applies. In providing access, CPRA remains mindful of individual privacy rights.

Campus Privacy Official: The individual at each location responsible for overseeing the strategic direction and application of the UC Statement of Privacy Values & Privacy Principles² and UC Privacy Balancing Process.

Commercial Purposes: Any purpose that has financial gain as a major objective.

Family Educational Rights and Privacy Act (FERPA): The federal law that addresses the privacy of students' educational records, which are records directly related to a student and are maintained by the University or a party acting for or on behalf of the University.

General Data Protection Regulation ("GDPR"): A privacy law of the European Union that governs the use of personally identifiable information. It concerns the personal data of individuals in the European Economic Area (EEA), which includes EU countries as well as the United Kingdom, Iceland, Norway, and Lichtenstein. The GDPR defines "personal data" very broadly such that the term includes names, addresses, phone numbers, national IDs, IP addresses, profile pictures, personal healthcare data, educational data, and any other data that can be used to identify an individual. It addresses multiple issues, such as the rights of data subjects, consent, and purpose of use.

Information Practices Coordinator: The individual at each location responsible for administering responses to records requests, and providing guidance to constituents at their locations on matters related to the access, use, and disclosure of information maintained in Administrative Records.

Information Privacy: As defined in the UC Statement of Privacy Values & Privacy Principles, is the appropriate protection, use, and dissemination of information about individuals.

¹ Administrative records do not include the records held by the Principal Officers of The Regents; teaching and research records (e.g., library materials, faculty research and teaching materials, student examinations); or records pertaining to individual patient care (medical records).

² For more information, see Section IV.C. Roles and Responsibilities. A list of current privacy officials can be found at <http://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/campus-privacy-officials.html>.

Mailing Lists: Any compilation of names and addresses, including email addresses.

Personally Identifiable Information (PII): Any information that describes or identifies an individual, including but not limited to name, Social Security number, physical description, home address, telephone numbers, email address, education, financial matters, medical or employment history, or statements made by or attributed to the individual.

Privacy and Information Security Board: The privacy and information security board at each location that advises on privacy and information security; sets strategic direction for autonomy privacy, information privacy, and information security; champions the UC Privacy Values & Privacy Principles, and the UC Privacy Balancing Process; and monitors compliance and assesses risk and effectiveness of location privacy and information security programs. These boards may be separate committees or structured as part of an existing location governance committee.

Records Management Coordinator: As defined in RMP-1, the individual at each location responsible for the development, coordination, implementation, and management of the Records Management Program at the location.

Records Management Program: In accordance with RMP-1, the Program that promotes sound, efficient, and economical records management in the following areas: (1) creation, organization of, and access to records; (2) maintenance and retention of Administrative Records; (3) security and privacy of records; (4) protection of records vital to the University; (5) preservation of records of historical importance; (6) disposition of Administrative Records when they no longer serve their purpose; and (7) other functions the University may deem necessary for good records management.

Student Applicant Records: Records of a person during the period of application, acceptance, and admission to the University, *prior* to enrollment.

Telephone Directories: A collection of individuals' names, telephone numbers, and other contact information, including employee (campus) or student directories.

UC Privacy Balancing Process: The process designed to address privacy risks when there is no policy in place pertaining to the situation.³

III. INTRODUCTION

~~On June 12, 1978, the Vice President—Academic and Staff Personnel Relations issued guidelines for implementing recently enacted legislation related to privacy of and access to University records. As stated in those guidelines it was necessary to implement a series of information practices requirements, including the following:~~

³ See UC Privacy and Information Security Steering Committee Report to the President January 2013, page 18

- ~~—restrict the use of Social Security numbers; (Federal Privacy Act of 1974);~~
- ~~—provide for access by the public to all University records, other than litigation, law enforcement, examination, property, library and museum, and certain personnel and medical records, or records whose disclosure is prohibited by law (California Public Records Act);~~
- ~~—withhold from public access those records for which it can be demonstrated that the public interest served by not making the record public clearly outweighs the public interest served by disclosure of the record (California Public Records Act);~~
- ~~—assure that personal information will not be disclosed unless the disclosure meets one or more of fourteen specific exceptions (Information Practices Act of 1977/IPA);~~
- ~~—establish procedures which ensure that individuals may inquire and be notified whether the University maintains records about them and may inspect those records (with certain exceptions); such procedures to be consistent with eleven criteria (IPA);~~
- ~~—maintain only that information which is pertinent and necessary to accomplish a purpose of the University or is authorized by law (IPA);~~
- ~~—provide with any form used to collect personal information eight specific items of information, such as the principal purpose for which the information is to be used and whether submission of information requested is voluntary or mandatory (IPA);~~
- ~~—assure that mailing lists meet certain standards for protecting the privacy of individuals (IPA);~~
- ~~—establish procedures for recording certain types of disclosures, and correcting such disclosed information (IPA); and~~
- ~~—provide the State Office of Information Practices with a detailed inventory of University records containing personal information (IPA).~~

These requirements are still valid. However, records management procedures and responsibilities have evolved through the practical application within the University of the referenced privacy and access laws. This Bulletin incorporates and therefore supersedes the June 12, 1978 guidelines, and sets forth applicable procedures and responsibilities.

III. POLICY TEXT

This policy applies to all Personally Identifiable Information (PII) in the University of California's Administrative Records, regardless of the record's function or medium, and addresses requirements related to the treatment of such information. Requests for academic

personnel records from government agencies are governed by Business and Finance Bulletin Records Management and Privacy Policies 9a, 9b, and 9c.⁴

All faculty, staff, and other individuals associated with the University who have access to Administrative Records containing PII must understand their responsibilities for safeguarding the privacy of that information. The Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators in consultation with the UC Office of the General Counsel (OGC), are responsible for providing overall policy and procedural guidance to University locations about privacy of and access to Administrative Records.⁵

A. Rules of Conduct for Employees with Access to Information Concerning Individuals

The University of California requires employees to adhere to the following rules of conduct concerning minimum standards⁶ for the collection, maintenance, disclosure, safeguarding, and destruction of Administrative Records containing PII. The California Information Practices Act (IPA) requires that any officer or employee who intentionally violates this policy, including these rules of conduct, may be subject to discipline, up to and including termination.⁷

1. Employees responsible for the collection, maintenance, use, and dissemination of Administrative Records that contain PII, must comply with the provisions of the IPA.
2. Employees must not require individuals to disclose PII about themselves or others that is not necessary and relevant to the purposes of the University or to the particular function for which the employee is responsible.
3. Employees must make every reasonable effort to ensure inquiries and requests by individuals for records containing their PII are responded to quickly, courteously, and without requiring the requester to repeat the inquiry to others unnecessarily.
4. Employees must assist individuals seeking information pertaining to themselves with making their inquiries sufficiently specific and descriptive to facilitate locating the records.
5. Employees must not disclose PII to unauthorized persons or entities.
6. Employees must not seek out or use PII relating to others for their own interest or advantage.

⁴ For additional requirements concerning requests for and access to academic peer review records, see policy APM-160.

⁵ For more information about the specific responsibilities of each role, see Section IV.C.

⁶ See Rules of Conduct for University Employees Involved with Information Regarding Individuals, part of the Privacy Principles and Practices at UC

⁷ California Civil Code § 1798.55

7. Employees responsible for the maintenance of records containing PII must take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the records from unauthorized access, use and disclosure.

B. Management of Records containing PII

For specific procedures concerning mailing lists and student records including application records, see Section VI Procedures. For information concerning academic peer review records, see APM-160.

The University strives to collect and maintain only information that is necessary and pertinent to accomplish its University mission.

To the greatest extent practicable, information about an individual must be collected directly from the individual to whom it pertains. When this is not possible, the University must maintain the source or sources of information, in a readily accessible format, in order to provide the source or sources to the individual upon request. When PII is disclosed, individuals may be notified according to existing legal requirements, University policy, and campus practices.

Each location must establish procedures that ensure an individual's right to inquire and be notified whether the University maintains records about them; and provide the records for inspection by the individual to the extent required by law. These procedures must be consistent with the requirements of the IPA, and University policies, such as UC IS-3 Electronic Information Security.

1. Use of PII for Commercial Purposes

The University prohibits employees responsible for maintaining or accessing records with PII from distributing, selling, or renting PII for commercial purposes unless such action is specifically authorized by law.⁸

2. Disposition of Administrative Records Containing PII

Information held by the University must be disposed of in accordance with federal and state law, and as required by RMP-2 Records Retention and Disposition and the UC Records Retention Schedule, unless it is needed as evidence in an investigation, foreseeable or on-going litigation, on-going audit, on-going records request or other special circumstance – in which case the information must be retained until these actions have been completed or resolved.

3. Procedures for Reporting Unauthorized Disclosures or Breaches of PII

⁸ For example California Civil Code §1798.60

Each location is responsible for developing its procedures for reporting unauthorized disclosures or breaches of PII for both paper and electronic records. Procedures for reporting electronic unauthorized disclosures or breaches of PII must be consistent with the University of California Privacy and Data Security Incident Response Plan.

4. General Data Protection Regulation (“GDPR”) Requirements

GDPR requirements may be more restrictive and UC guidance for it must be consulted.

C. Evaluating Use or Disclosure of PII

When neither law nor policy provides definitive guidance regarding a proposed use or disclosure of PII, the University must use the UC Privacy Balancing Process to adjudicate privacy and other competing interests.

Under the Balancing Process, the University must not make public disclosures of information when it can demonstrate that the public interest served by nondisclosure clearly outweighs the public interest served by disclosing the information. In reaching this decision, the University must review specific statutory exceptions that might allow for disclosure of PII. Situations involving unprecedented and significant balancing concerns are referred to the location’s Privacy Board unless a relevant alternative adjudication path is already established.

IV. COMPLIANCE / RESPONSIBILITIES

A. Implementation of the Policy

The Vice President for Information Technology Services and Chief Information Officer is responsible for issuing and updating any requirements, standards or guidelines that support this policy.

Chancellors, the Vice President of Agriculture and Natural Resources, and UC Managed Laboratory Directors are responsible for designating an Information Practices Coordinator, Campus Privacy Official, and Records Management Coordinator to administer and implement this policy at their location.

The UC Information Practices Coordinator, UC Privacy Manager, and UC Records Manager facilitate regular communication among local Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators to address consistent implementation of this policy throughout the University. Each Information Practices Coordinator, Privacy Official, and Records Management Coordinator must work together at their locations to ensure consistent implementation of this policy, as necessary.

IV. RESPONSIBILITIES

A. University-wide Responsibility

The Senior Vice President—Administration has major responsibility for University-wide compliance with legal requirements on privacy of and access to University records. Within that organization, the Coordinator of Information Practices and Special Projects, in consultation with General Counsel as appropriate, provides overall records privacy and access policy and procedural guidance to campuses, Laboratories, and offices of the President, as well as liaison with the State Office of Information Practices.

B. Campus, Laboratory, and Office of the President Responsibilities

1. Chancellors, Laboratory Directors*, the Vice President—Agriculture and Natural Resources, and the Senior Vice President—Administration responsible for ensuring that departments and other units under their respective jurisdictions comply with all records privacy and access requirements. To facilitate this responsibility, and because of the complexity of the task of implementing access and privacy requirements and the likelihood of lawsuits if requirements are not met, each of these officers appoints a senior officer as Coordinator of Information Practices:

*Los Alamos National Scientific Laboratory is expected to comply with all policy and procedural requirements for privacy of and access to information, although it should be understood that the Civil Remedies and Penalties section of the State of California Information Practices Act and Public Records Act may not be applicable in New Mexico.

2. The local Coordinators of Information Practices are responsible for developing privacy and access guidelines, as well as providing technical and practical assistance to all offices at their locations. To assure that local records procedures and practices are consistent with University policies and Federal and State laws, the Coordinators are responsible for liaison with the Office of the President Coordinator of Information Practices and Special Projects. In fulfilling these responsibilities, local Coordinators shall:

- understand legal requirements, including the differences between confidential, personal, and non-personal information;
- prepare a yearly inventory of personal and confidential records systems for ultimate transmittal to the State; and
- periodically review record systems to ensure that files are maintained with accuracy, relevance, timeliness, and completeness.

The local Coordinators should provide guidance to their constituencies which:

- ensures that local forms requesting or providing personal or confidential information have privacy notices incorporated in them or attached to them;
- ensures that individuals have access to information about themselves unless the information has been determined to be confidential;

~~—ensures that individuals may amend a record about themselves and that appropriate action is taken within specified time periods and in accordance with University and legal requirements;~~

~~—establishes charges, if any, for copies of any records to which individuals are entitled to have access, and ensure that such charges are in accordance with University and legal requirements;~~

~~—establishes records of disclosure of information if required by an existing State statute;~~

~~—assure the security of files;~~

~~—allows disclosure of personally identifiable information to a non-profit educational institution conducting scientific research providing there is satisfactory determination of the need for personal or confidential information, a procedure for protecting the confidentiality of the information, and assurance that the personal identity of the subject shall not be further disclosed in individually identifiable form; and~~

~~—ensures that no information in a file is transferred inside or outside the University unless the transfer is consistent with legal requirements.~~

B. Revisions to the Policy

The Vice President for Information Technology Services and Chief Information Officer has the authority to initiate policy revisions and is responsible for regular reviews and updates consistent with approval authorities and applicable Bylaws and Standing Orders of The Regents.

C. Roles & Responsibilities

The following functions are critical to ensuring the University handles information in a manner consistent with the University's legal obligations, policy requirements, and the UC Statement of Privacy Values & Privacy Principles. Together, Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators serve as subject matter experts and collaborate with other disciplines to strengthen the University's information governance framework.

1. University Employees

All faculty, staff, and other University community members with access to records with PII must safeguard the records from unauthorized access, use and disclosure.

2. University Managers

All managers must ensure that any personnel who have access to records with PII are made aware of their responsibilities for handling such records, including protecting the records from unauthorized access, use and disclosure.

3. Information Practices Coordinators

The Information Practices Coordinator at each location is responsible for administering responses to records requests, and providing guidance on matters related to the access, use, and disclosure of information maintained in Administrative Records. The California Public Records Act (CPRA) Office within the OGC provides guidance to campuses and may manage multi-campus CPRA requests on behalf of the locations. At their locations, Information Practices Coordinators also:

- i. Ensure that procedures and practices for access, amendment, use and disclosure of Administrative Records adhere to federal and state laws, including but not limited to the IPA and the CPRA.
- ii. Develop guidelines, including training programs, on IPA and CPRA practices, including the rules of conduct outlined in Section III.A.
- iii. Review local PII collection and notice practices upon request.
- iv. Assist with interpretation of federal and state privacy and disclosure laws and University policies including but not limited to the CPRA, IPA and the UC rules of conduct outlined in Section III.A.

4. Campus Privacy Officials

Campus Privacy Officials at each location are responsible for overseeing the strategic direction and application of the UC Statement of Privacy Values & Privacy Principles, and UC Privacy Balancing Process throughout the activities at that location.

5. Records Management Coordinators

As defined in RMP-1, Records Management Coordinators are responsible for the development, coordination, implementation, and management of the Records Management Program at their locations.

6. Chancellors, the Vice President of Agriculture and Natural Resources, and UC Managed Laboratory Directors

These positions are responsible for designating an Information Practices Coordinator, Campus Privacy Official, and Records Management Coordinator to administer and implement this policy at their locations.

7. The Vice President for Information Technology Services and Chief Information Officer

This position is responsible for issuing and updating any requirements, standards or guidelines that support this policy.

V. PROCEDURES

For specific categories of PII, all locations must follow the procedures below to ensure consistency across the University.

NUMBER RMP 11

Formatted: Highlight

STUDENT APPLICANT RECORDS

EFFECTIVE DATE

June 15, 1989

REFER ALL SYSTEMWIDE QUESTIONS TO:

Blank

REFER ALL CAMPUS QUESTIONS TO:

Blank

I. REFERENCES

Business and Finance Bulletin RMP 8, "Legal Requirements on Privacy of and Access to Information," dated December 10, 1985, with revised pages 5, 22, and 28 dated September 15, 1986; revised page 8 dated February 1, 1987; revised pages 2, 8a, 9-12, 18, 18a, and 19-23 dated April 15, 1988; and revised pages 14 and 15 dated February 15, 1989.

Letter from Afton E. Crooks, Coordinator of Information Practices and Special Projects, Office of the President, to Olga Euben, Associate Director of Admissions, Santa Cruz campus, August 24, 1982.

Letter from A. T. Brugger, Special Assistant for Student Affairs Services, Office of the President, to Edward Birch, Vice-Chancellor, Student and Community Affairs, Santa Barbara campus, June 27, 1983.

Letter from Rosalie G. Passovoy, Coordinator of Student Special Services, Office of President, to Masa Fujitani, Associate Director of Admissions, Irvine campus, July 1, 1983.

Letter from Vice-Chancellor Birch to Charles W. McKinney, Registrar and Robert E. Bason, Assistant Chancellor University Relations, Santa Barbara campus, September 8, 1983.

Letter from Coordinator Passovoy to Michael Miller, Director of Student Recruitment, Riverside campus, September 14, 1984.

Letter from Coordinator Crooks to Director Miller, January 18, 1985.

Letter from Philip E. Spiekerman, University Counsel, Office of the General Counsel, to Virginia Kelsch, Associate Director of Development, University Advancement, Irvine campus, June 21, 1985.

Opinion by Melvin W. Beal, University Counsel, Office of the General Counsel, to Jack W. Peltason, Chancellor, Irvine campus, July 30, 1985.

California State Information Practices Act, Section 1798 et seq.

II. INTRODUCTION AND DEFINITIONS

The purpose of this Bulletin is to furnish guidelines for consistent and fair practices in providing and protecting access to records of University applicants (as distinct from full-fledged, matriculating students) in accordance with applicable laws and University policies.

[Found in the beginning of the new RMP-7, under Definitions:]

Student Applicant Records: Records of a person during the period of application, acceptance, and admission to the University, *prior* to enrollment.

A. Applicant Records reference a person during the period of application, acceptance, and admission to the University, *prior* to actual enrollment in classes.

A. Student Applicant Records

In accordance with California law, the University only collects information relevant to the University's purposes. Disclosure of this information must be in accordance with state and federal law.

Until an applicant has enrolled in an academic program, any records referring to them are considered student applicant records and must be used and accessed in a manner consistent with the protections afforded by the IPA.

Access to applicant records is governed by the State of California Information Practices Act (IPA). No distinction is made between U.S. and foreignborn student applicants regarding disclosure of information. The IPA protects the rights of individuals without regard to nationality.

B. Student records are those records which: (a) are directly related to a student, and (b) are maintained by a University of California campus or by a party acting for the campus, whether recorded by handwriting, print, tapes, film, microfilm, or other means. Student records include, but are not limited to, academic evaluations, transcripts, test scores and other academic records, general counseling and advising records, disciplinary records, and financial aid records. Applicant records become student records after the student has been admitted, enrolled in, and been in attendance, at the University. Access to student records is governed by the Federal

Family Educational Rights and Privacy Act (FERPA) and the State's Donohoe Act, as reflected in the University's Policies Applying to Campus Activities, Organizations, and Students, Part B.

Records directly related to an enrolled student, including the student's applicant records, are subject to the Family Educational Rights and Privacy Act (FERPA).⁹

III. CREATION, MAINTENANCE, AND DISPOSITION

The offices of the Graduate and/or Undergraduate Admissions are respectively responsible for creating, maintaining, and safeguarding access to applicant records.

The IPA allows for the collection only of information that is "relevant and necessary" to accomplish the intended stated purpose. In the case of applicant records, the information collected must clearly aid the University in determining eligibility for admission and ranking for scholarships, and disclosure of any allowable portion of it must be in accordance with the IPA (see Section IV, below).

The IPA further requires the application forms to carry a privacy notice and statement advising the person filling out the form whether answering the questions posed is mandatory or voluntary; what authority authorizes maintenance of the information; and what, if any, consequences exist for failure to supply any part of the information asked.

The University of California Records Disposition Schedules Manual provides specific guidelines as to how long admissions records are to be kept and when they should be destroyed. Copies of the Manual may be obtained from the campus or Office of the President Records Management Coordinators.

IV. DISCLOSURE GUIDELINES

Disclosure of applicant information is governed by three basic tenets:

(1) there are broad access rights by an individual to information pertaining to that individual; (2) nonpersonal information may be disclosed to anyone; and (3) disclosure to third parties of personal information is allowed only under specific statutory provisions.*

* See Business and Finance Bulletin RMP 8, "Legal Requirements on Privacy of and Access to Information," pp. 13-15, for definitions of personal and nonpersonal information, and pp. 18a-21 regarding disclosure. See also, July 30, 1985 letter from University Counsel Beal to Chancellor Peltason.

The following are guidelines which have been developed in response to specific questions regarding information from applicant records. While it is recognized that there are many more than the four categories herein addressed, the most frequently occurring questions over the years have involved these specific groups. We, therefore, have limited the discussion to them at this time.

⁹ For policy requirements and further information about privacy and potential disclosure of student records, please read Policies Applying to the Disclosure of Information from Student Records (UC PACAOS-130)

A. Applicants

~~In accordance with University policy, an applicant has the right to see records referencing him or her with regard to the application process, except that disclosure of evaluation forms and records in an applicant's file, "created with the documented understanding of confidentiality" is protected.~~

~~When the applicant is outside the U.S., a person representing the individual within the U.S. may be granted the same access rights to personal information regarding the applicant as those afforded the applicant, consistent with the IPA, Section 1798.24 (e).~~

An applicant has the right to inspect records that reference them in relation to the application process, and are maintained in the applicant's file, with the exception of recommendation letters and associated records created with the documented understanding of confidentiality.¹⁰

When the applicant is outside the United States, they may have a person within the U.S. act as their representative. This representative has the same right of access to the applicant's file. The University may disclose information to this representative if records within the University's possession demonstrate with reasonable certainty that this is the applicant's intended representative.

B1. Parents of Applicants

~~In accordance with the IPA, the University must not release information from the applicant's records to the applicant's parents and as a matter of University policy, information from the applicant's files is not released to parents of applicants without the applicant's written consent, regardless of the individual's age or financial status. The University's current Current admissions process provides forms provide the opportunity to furnish this consent.~~

In accordance with FERPA, the University must not release student records (including application records) to parents without the student's written consent, regardless of age or financial status, unless such release falls under a specific exception under FERPA.

2. Third Parties

~~In accordance with state law, the University may disclose PII about a University applicant to certain third parties (e.g., high school counselors). This information may include C. School Administrators and Teachers~~

~~According to University policy and the IPA, such personal information about a University applicant as eligibility status or lack of certain grades. The University may disclose this information may be disclosed to such third parties as school counselors only if:~~

- ~~a. The applicant gives prior written consent;~~
- ~~1. prior written consent is given by the applicant; or~~

¹⁰ California Civil Code §1798.38; 20 USC § 1232a(a)(1)(C)

~~b. The 2. the~~ information is necessary for performance of the third party's counselor's official duties, and its use is will be compatible with its original collection purpose; ~~or~~

~~c. The 3. the~~ requested information will be is to be used for scientific or statistical research and assurances of confidentiality and protection of personal identity are guaranteed, as per Section 1798.24 (u) of the IPA.; or

d. Other legal exceptions apply.

~~D3.~~ Advancement, Development, and Alumni Office Staff

Advancement, Development, and Alumni office staff have legitimate educational interest in applicants' records. These offices may access applicant information, including PII, when the information is relevant and necessary to carry out their assigned duties and is clearly related to the purpose In order to be accessed, the requested admissions records must clearly pertain to non-students and fall under the IPA definition of nonpersonal. IPA provisions for intra-agency disclosures prohibit disclosure of personal information unless such disclosure is "relevant and necessary" to carry out assigned duties, and is clearly "related to the purpose" for which the information was originally collected.

RMP-12 Guidelines for Assuring Privacy of Personal Information in Mailing Lists and Telephone Directories

Formatted: Highlight

June 15, 1989

I. REFERENCES

Civil Code Section 1798 et. seq., the Information Practices Act of 1977 (IPA).

Government Code Section 6250 et seq., the California Public Records Act (PRA).

Federal Family Educational Rights and Privacy Act of 1974 (FERPA).

The Donohoe Higher Education Act of 1977, Education Code, Sections 67100—67175.

University Policy Applying to the Disclosure of Information from Student Records, (Part B) Sections 10.00—11.30.

Business and Finance Bulletin RMP-8, "Legal Requirements on Privacy and Access to Information."

Business and Finance Bulletin BUS-65, "Guidelines for University Mail Services."

Policy Prohibiting Commercial Advertising in Official University Publications, issued by President David S. Saxon to Chancellors, Laboratory Directors, and Deans, April 12, 1979

~~Letter from President David P. Gardner to Chancellors, Laboratory Directors, and Deans, July 26, 1985, reaffirming the April 12, 1979 policy.~~

~~Letter from Afton E. Crooks, Coordinator of Information Practices and Special Projects, Office of the President to Warren E. Schoonover, Director of Agriculture and Natural Resources, Office of the President, January 30, 1986.~~

~~Letter from Susie Castillo Robson, Coordinator of Student Records, Office of the President, to Sue Carberry, Coordinator of Information Practices, Santa Barbara Campus, regarding the commercial use of public information contained in student directories, March 10, 1986.~~

~~II. INTRODUCTION~~

~~The Information Practices Act (IPA) requires that protection of the individual's right to privacy be given consideration in all aspects of University Business.~~

~~The University's obligation to promote its purposes and communicate efficiently with employees, students, and others on University business makes it desirable to produce and maintain directories and mailing lists which include individuals' names, campus or business addresses and telephone numbers, and certain items of personal information about those individuals.~~

~~The purpose of this Bulletin is to:~~

- ~~A. describe the types of mailing lists and directories the University maintains;~~
- ~~B. clarify the circumstances under which personal information may or may not be included in them, and~~
- ~~C. establish guidelines for subsequent distribution and use.~~

~~Except where noted in Sections I. and V.B.2, this Bulletin will deal only with mailing lists and telephone directories that are not governed by federal and state law and University policies relating to information contained in student records maintained by the University.~~

~~III. LEGAL REQUIREMENTS~~

~~A. Confidentiality of Home Address and Telephone Number~~

~~According to Government Code Section 6254.3 (PRA), the home addresses and telephone numbers of state employees are not deemed to be public records and cannot be released without written permission of the individual.~~

~~B. Notification of Intended Use of Personal Information~~

~~Civil Code Section 1798.17 (IPA) provides that the individual will be notified of the intended purpose and use of personal information being collected. Periodic updating of that notification shall occur at not more than one-year intervals.~~

~~C. Prohibition on Release of Names and Addresses for Commercial Purposes~~

~~Civil Code Section 1798.60 (IPA) prohibits distribution, rental, or sale of an individual's name and address for commercial purposes unless specifically authorized by law.~~

~~D. Removal of Names from Mailing Lists~~

B. University Mailing Lists and Telephone Directories

Upon written request from any individual, any University office that maintains a Mailing List must remove that individual's name and address from such list, unless the list is used by the University solely for necessary direct contact with the individual.

The University must not use or disclose its Telephone Directories and Mailing Lists for commercial purposes, unless such action is specifically authorized by law.

~~Civil Code Section 1798.62 (IPA) gives individuals the right, upon written request, to have their own name and address removed from any agency list, unless that list is used exclusively for the purpose of directly contacting the individual.~~

IV. LEGAL DEFINITIONS

A. Commercial Purposes

~~Civil Code Section 1798.3 (j):~~

~~"The term 'commercial purposes' means any purpose which has financial gain as a major objective."~~

B. Personal Information

~~Civil Code Section 1798.3 (a):~~

~~"The term 'personal information' means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history."~~

~~The types of personal information typically found in mailing lists and directories that are the subject of this Bulletin are not limited to, but might include an individual's home address and telephone number, marital status, and spouse's name.~~

Further definition and explanation regarding personal information can be found in Section VII.B., on page 15 of Business and Finance Bulletin RMP-8, "Legal Requirements of and Access to Information".

V. GENERAL DEFINITIONS

[Found in the beginning of the new RMP-7, under Definitions:]

~~A. **Mailing Lists:** A mailing list is any compilation of names and addresses, including email addresses. Further information regarding mailing lists may be found in Section IV.C. of Business and Finance Bulletin BUS-65, "Guidelines for University Mail Services".~~

~~B. **Telephone Directories:** A collection of individuals' names, telephone numbers, and other contact information, including employee (campus) or student directories.~~

~~1. Employee (campus) directories: Typically include the employee's name, department and title, campus address, and telephone. Campus directories may also include the employee's home address and telephone as well as spouse's name.~~

~~2. Student directories: Typically include the student's name, campus address, local telephone number, and home address. Student directories are compiled from student records, which are subject to different legislative requirements from all other University records. Student records are governed by:~~

~~a. the Federal Family Educational Rights and Privacy Act of 1974 (FERPA);~~

~~b. University policy, and~~

~~c. certain sections of the California Education Code adopted by The Regents of the University.~~

~~Questions regarding student records, or any publications compiled from student record information, should be directed to the Assistant Vice President Student Academic Services, Office of the President.~~

~~C. University Publications~~

~~President Saxon's policy statement of April 12, 1979 defines official University publications as those that are informational or administrative, and used in the conduct of routine activities. Examples include: maps, guides, directories, catalogues, departmental announcements, and class schedules.~~

VI. PROCEDURES

~~A. Collecting Personal Information for Inclusion in Telephone Directories and Mailing Lists~~

1. Written voluntary consent from each individual is required before any personal information may be included in any list or directory maintained by the University.

2. Forms used to collect personal information for inclusion in a University directory or mailing list must include the standard State privacy notice explaining its intended use, unless the directory or mailing list is to be used only by the University for the purpose of communicating with the individual.

B. Complying with the IPA

1. To comply with the IPA, a notice similar to the following shall be printed in each directory:

"This campus directory is the property of the University of California (campus name). To protect the privacy of individuals listed herein, in accordance with the State of California Information Practices Act, this directory may not be used, rented, distributed, or sold for commercial purposes."

2. When a form used to collect personal information includes a 'yes-no' box to be checked, or a signature line indicating consent to release the information being collected, any line or box inadvertently or purposely left blank must be interpreted as a statement of "non-consent". Records of consent or non-consent must be updated annually to comply with provisions of the IPA.

3. Individuals may request in writing to have a name removed from any specified mailing list. However, the University is not obligated to remove a name if the list is used exclusively to notify the individual, or for some other official University purpose.

C. Complying with University Policy

1. President Saxon's 1979 letter defines 'official publication' and states that such a publication 'should not contain commercial advertising'.

2. President Gardner's 1985 letter reiterates and confirms the 1979 ruling prohibiting commercial advertising in official University publications such as directories and mailing lists.

V. RELATED INFORMATION

Academic Personnel Manual

- Section 160, Maintenance of, Access to, and Opportunity to Request Amendment of Academic Personnel Records

Business and Finance Bulletins

- [IS-3, Electronic Information Security](#)
- [RMP-1, University Records Management Program](#)
- [RMP-2, Records Retention and Disposition](#)
- [RMP-9a, -9b, -9c, Guidelines for Access to University Personnel Records by Governmental Agencies](#)

[Personnel Policies for Staff Members](#)

- [PPSM 21, Selection and Appointment](#)

[Federal and State Laws](#)

- [California Constitution, Article I, Section 1 and 3](#)
- [California Information Practices Act](#)
- [California Public Records Act](#)
- [Family Educational Rights and Privacy Act](#)

[Other Presidential Policies and Guidelines](#)

- [Electronic Communications Policy](#)
- [Gramm-Leach-Bliley Compliance Plan](#)
- [UC Policy on Public Disclosure of Compensation Information](#)
- [UC Privacy Balancing Process](#)
- [UC Privacy and Data Security Incident Response Plan](#)
- [UC Privacy and Information Security Steering Committee Report to the President January 2013](#)
- [UC Statement of Privacy Values & Privacy Principles](#)

[Other](#)

- [UC Procurement Appendix DS — Data Security and Privacy](#)

[For specific additional requirements about Student Records, Protected Health Information \(PHI\), and Academic Peer Review Records please refer to the policies below:](#)

- [Student Education Records: UC PACAOS-130 Policies Applying to the Disclosure of Information from Student Records and the Federal Family Educational Rights and Privacy Act \(FERPA\) primarily govern the handling of student education records.](#)
- [Protected Health Information: The University's HIPAA policies, the Health Information Portability and Accountability Act of 1996 \(HIPAA\), and subsequent amendments in the Health Information Technology for Economic and Clinical Health \(HITECH\) Act govern the handling of Protected Health Information.](#)

- Academic Peer Review Records: See APM 160-20
This policy defines the rights of individuals and entities to have access to academic peer review records.

VI. FREQUENTLY ASKED QUESTIONS

Not applicable

VII. REVISION HISTORY

Revision Date: This Policy was remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

This policy replaces the following policies:

- BFB-RMP-7: Privacy of and Access to Information Responsibilities. November 1, 1985 Initial Version.
- BFB-RMP-8: Requirements of Privacy of and Access to Information. November 13, 2015 Rescinded.
- BFB-RMP-11: Student Applicant Records. June 15, 1989 Initial Version.
- BFB-RMP-12: Guidelines for Assuring Privacy of Personal Information in Mailing Lists and Telephone Directories. June 15, 1989 Initial Version



Principles of Accountability with Respect to Financial Transactions

Responsible Officer:	AVP - Systemwide Controller
Responsible Office:	FO - Financial Operations
Issuance Date:	[Issuance Date]
Effective Date:	<u>2/23/2016</u>
Last Review Date:	<u>August _____, 2015</u>
Scope:	<p>This policy applies to any person working for or conducting business on behalf of the campuses, medical centers, Office of the President, and Agriculture & Natural Resources.</p> <p>This policy does not apply to Lawrence Berkeley National Laboratory (LBNL).</p>

- I. POLICY SUMMARY** _____ **1**
- II. DEFINITIONS** _____ **2**
- III. POLICY TEXT** _____ **2**
- IV. COMPLIANCE / RESPONSIBILITIES** ___ **7**
- V. PROCEDURES** _____ **9**
- VI. RELATED INFORMATION** _____ **16**
- VII. FREQUENTLY ASKED QUESTIONS** __ **16**
- VIII. REVISION HISTORY** _____ **16**

Contact:	<u>Ruth Satorre</u>
Title:	Director Corporate Accounting
Email:	Ruth.Satorre@ucop.edu
Phone #:	(510) 987-0414

I. POLICY SUMMARY

This policy provides an overview of financial accountability, financial management, data integrity, and compliance associated with financial transactions throughout the

University. Campuses should develop policies and procedures to ensure these financial transaction accountability principles are met.

II. DEFINITIONS

Financial stewardship is defined as the responsibility for managing University resources wisely and executing these responsibilities with integrity and ethical conduct. These resources include time, money, people and property. When University employees manage public resources in an efficient, economical and ethical manner, the result will be better achievement of the University's overall missions of teaching, research and public service. Financial stewardship includes the responsibility for establishing and monitoring the system of internal control.

III. POLICY STATEMENT

A. Background

Under [Regents Standing Order 100.4: Duties of the President of the University](#), certain duties are delegated to the President, including the authority to redelegate any of the duties of the office, except service as an ex officio Regent.

The President redelegated certain duties to the campuses such as the authority to execute contracts, agreements and to sign checks. For a list of duties redelegated by the President, please see the [delegation authority index](#).

The Chancellors have redelegated certain authority to departments and schools to initiate transactions. This policy outlines the requirements for individuals who have been delegated the authority to process financial transactions.

The dean or manager of each school or department, while responsible for managing the department's financial resources, will normally delegate the overall financial management administration to a Department Administrator (DA).¹ The DA is responsible for developing an appropriate structure for handling the department's financial resources. The DA should consider whether to divide or segregate the tasks among different people to reduce the risk of error or inappropriate or fraudulent actions. Segregating the tasks require dividing the responsibility for recording, authorizing, and approving transactions, and handling the financial resources.

B. Financial Management

1. Monitoring and Evaluating Financial Data

¹ If financial management administration is already delegated to centralized administrative units (*outside* the departments), then the department **should not** delegate its financial resource management unless there is an overriding business need to do so.

Commented [JE1]: Should give a definition in the "definition section". This could mean on a campus thousands of individuals orbased on an interpretation

RAS – Definition not needed (it seems to be laid out pretty clearly here as someone that assists in executing the management of the department's financial resources).

Each department head and DA must establish monitoring procedures to provide assurance that financial transactions ~~are appropriate and~~ are accurately recorded and comply with applicable regulations, policies, etc.

C. Data Integrity

1. Managing University Data

Financial management decisions affect every aspect of the University, but such decisions can only be as good as the data on which they are based. Consequently, each department must establish and implement procedures to ensure data integrity ~~supporting transaction processing~~. These procedures must be documented and provide reasonable assurance that transactions are valid, ~~in accordance with management's authorization~~ supported by proper documentations and ~~are~~ recorded in an accurate and timely manner in the University general ledger.

2. Establishing Separation of Duties Controls for Data Integrity

No single individual shall have complete control over all processing functions for any financial transaction. If the number of employees in a department is limited, causing one person to perform multiple functions, the department must assign a second person to review the work for accuracy, completeness and timeliness, or combine these functions with another unit.

3. Departmental Computing Responsibilities

Each department needs experienced and well-trained technical professionals to support the department's computing needs. Such support can be contracted for or provided by a department itself through the IT department.

If a department is developing or acquiring information systems for their use, the requirements in [IS-10](#), *Systems Development Standards* must be followed.

D. Compliance

Every employee who conducts transactions that affect University funds must understand and comply with all applicable laws, regulations, and special restrictions. To ensure compliance, each department head and DA shall adopt the following practices:

1. California State Oath of Allegiance

Departments will ensure that every University employee signs the *State Oath of Allegiance*, at the date of hire, but no later than the time at which the employee begins providing compensable service. For more

Formatted: Normal, Indent: Left: 1"

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

information, please see Accounting Manual Chapter [P-196-21](#), *Damage Payments for Services Performed Before Loyalty Oath Is Signed*, and [Campus Procedures and Frequently Asked Questions: Damage Payment for Services Performed before Loyalty Oath is Performed](#).

2. Financial Reporting

Departments will record transactions in compliance with applicable financial reporting requirements, including Generally Accepted Accounting Principles (GAAP), Governmental Accounting Standards Board (GASB) Statements, Cost Accounting Standards Board (CASB) Statements, and applicable policies and standards of the University, campuses, and medical centers.

Accounting principles must be applied consistently. Financial Management or like department at the campus and system wide levels are entrusted with ensuring consistent, University-wide application of these accounting principles.

Reports to sponsoring entities will be made according to the specific reporting requirements. In general, most sponsoring entities require adherence to GAAP. Additionally, federal agencies and entities which serve as conduits for federal funds require adherence to [2 CFR Part 200](#) - *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*.

3. Records Retention

Each DA will maintain financial records in compliance with regulatory requirements and University policy, including cases where there is pending litigation or audits, records must be maintained until the action is concluded. For more information on records retention, please refer to the local records management coordinators, [RMP-1](#), *University Records Management Program*, and [RMP-2](#), *Records Retention and Disposition: Principles, Processes, and Guidelines*.

4. Expenditures

All expenditures ~~and actions affecting a person's compensation~~ must comply with applicable regulatory and legal requirements and University policy.

All expenditures and Actions affecting a person's compensation must adhere to applicable regulatory and legal requirements and University policy.

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

5. Tax Laws and Regulations

To comply with tax regulations, each DA must ensure that appropriate personnel are informed of the various tax authority requirements applicable to their operations.

For more information, see the [University of California Sales & Use Tax Manual](#) and Accounting Manual Chapter T-182-73, *Taxes: Sales and Use Tax*.

6. Exemption from Property Taxes in California

The University is generally exempt from paying real and personal property taxes in California, as described in [G-38](#), *Tax Exemption and Refund Claims Filing for Property Leased by the University*. When necessary, the Facilities Management Department or other appropriate campus department will file the exemption reports and claims to receive refunds of such taxes paid on leased property for the departments.

7. Reporting Fraudulent or Illegal Acts

Any person who becomes aware of fraudulent or illegal business transactions conducted in the name of the University shall properly report the fraudulent or illegal act to the appropriate University official or workgroup. This includes:

- Any person who suspects that fraud or illegal activities are taking place in his or her department must report that suspicion immediately in accordance with the [University of California Whistleblower Policy](#).
- Individuals conducting business on behalf of the University are personally responsible for the consequences of any violations they commit.
- Individuals conducting business on behalf of the University must do so for the benefit of the University. Where a potential for personal gain exists, this potential conflict of interest must be reported immediately, and be carefully evaluated before any financial transactions are allowed to occur.

For complete guidance on reporting irregularities, see the [University of California Whistleblower Policy](#).

8. Response to External Audits from Regulatory Agencies

The Senior Vice President – Chief Compliance and Audit Officer must be immediately notified when the University receives notification of any audit

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

or review by an external regulatory agency. Communications from regulatory agencies, donors, or other entities concerning noncompliance with laws, regulations, applicable guidelines, directives or an appropriate standard of care must be disclosed in writing to the Associate Vice President-Systemwide Controller.

IV. COMPLIANCE / RESPONSIBILITIES

Function	Responsibilities
Associate Vice President-Systemwide Controller	<ul style="list-style-type: none"> Establish and update the policies set forth in this Bulletin.
Department Heads and Department Administrators (DAs)	<ul style="list-style-type: none"> <u>Understand all relevant regulatory requirements, the campus system, the University policies, and purpose of each transaction;</u> Develop an accountability structure; Ensure department manages financial resources in an efficient and cost-effective manner; Establish monitoring procedures to provide assurance that financial transactions are appropriate, and are accurately recorded <u>and comply with applicable regulations, policies, etc.;</u> Develop procedures to ensure data integrity; Conduct transactions in compliance with applicable financial reporting requirements; Maintain financial records in compliance with regulatory requirements and University policy; Departments that conduct sales activities must charge sales tax and properly account for sales tax collected; Departments making purchases must include a provision for sales and use taxes when making orders; Submit accurate and timely data to Campus Payroll Office, UC PATH and/or other appropriate department; Determine if individuals are employees or contractors for tax purposes; Have experienced and well-trained technical professionals to support the department's computing needs.
Preparer	<ul style="list-style-type: none"> Understand all relevant regulatory requirements, the campus systems, the University policies, and the purpose of each transaction; Enter accurate data into all fields on a transaction document or application system screen; Record an accurate and thorough explanation of each transaction; Ensure that the proper Full Accounting Units (FAUs) are entered; Ensure that any new account and fund linkages requested are appropriate; Be aware of basic policy, regulatory, and other requirements; Resolve any questions which come to mind during the completion of the transaction, or are raised via on-line edits and related messages; and Provide the completed transaction, with any supporting documents, to a Reviewer.
Reviewer	<ul style="list-style-type: none"> Review all transactions within a reasonable time; Inspect each transaction to ensure the Preparer properly fulfilled his

University of California – Policy [Policy Number]
 Principles of Accountability with Respect to Financial Transactions

Function	Responsibilities
	or her responsibilities; <ul style="list-style-type: none"> • Ensure that each transaction complies with policy, regulatory, and other requirements; • Resolve all questions that arise concerning a transaction, or ensure the transaction is reversed until the questions are resolved; • Notify the DA if he or she will be absent from work, so another Reviewer can be assigned; and • Notify the DA when he or she is returning to work from an absence.
Chief Procurement Officer, Authorized Buyers, or Specified University Departments	<ul style="list-style-type: none"> • Execute the purchases of: <ul style="list-style-type: none"> ○ Real estate and construction projects; ○ Services of independent consultants; and ○ Legal services.
Departments Engaged in Unrelated Business Income (UBI) Activities	<ul style="list-style-type: none"> • Maintain information supporting whether or not the income is taxable; • Complete UBI questionnaires and worksheets for UBI activities and send them to the appropriate Campus Tax Service Coordinator, who will review and forward them to UCOP Tax Services; and • Account for all taxable UBI earned in an income-producing fund approved by Corporate Accounting.
Campus Payroll Office, UC PATH, and/or other appropriate department	<ul style="list-style-type: none"> • Withhold and remit Federal and State taxes on compensation based upon the individuals' Form W-4; • Complete the required quarterly tax returns; • Distribute Forms W-2 to employees; • Report information on non-compensation payments to payees outside the University or University employees on annual reporting forms such as Forms 1099, W-2, or 1042-S.
Senior Vice President – Chief Compliance and Audit Officer	<ul style="list-style-type: none"> • Notified when the University receives notification of any audit or review by an external regulatory agency. • The delegation to an External Audit Coordinator depends on the type of external regulatory agency and the type of audit conducted.
Facilities Management Department or the appropriate campus department	<ul style="list-style-type: none"> • File the exemption reports and claims to receive refunds of such taxes paid on leased property for the departments.

V. PROCEDURES

A. Financial Principles

All employees with financial transaction authority re delegated to them should adhere to the following principles:

1. Accountability

Assigning responsibilities and maintaining information on activities so that they are traceable to the specific individual accountable for the transaction or activity.

Formatted: Heading 3, Indent: Left: 0", Space Before: 0 pt
 Formatted: Indent: Left: 1", Space Before: 0 pt

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

4-2. Authorization and approvals

Transactions should be approved and delegations of authority should be documented.

2-3. Documentation

Transactions should be supported by documentation and the transactions should comply with University policies.

3-4. Physical controls over assets

Physically secure assets (equipment, inventories, cash, checks, etc.) should be periodically counted and compared to the assets on record in accordance with UC Policy.

5. Controls over data

Limit data access to individuals whose duties are aligned with their need to access the data and protecting confidential information.

6-5. Management overrides

Prevent activities to circumvent controls or manipulate transactions, either intentionally or unintentionally.

7-6. Reconciliations

Ensure the completeness and accuracy of transactions and timely ~~investigate~~ investigation of any discrepancies.

8-7. Supervisory oversight

In conjunction with the fiscal close across all locations, University policy requires a signed "Fiscal Close Certification Letter" from those with fiscal responsibility. The letters are intended to enhance the level of integrity in the financial reporting process by demonstrating due diligence by those with fiscal responsibility. This letter is a component of a broader program to enhance the integrity in the fiscal closing process, ensure disclosures are adequate and provide an avenue for all relevant issues known by campus management to be considered by those responsible for signing the overall campus management representation letter signed by the Chancellors, Executive Vice Chancellors, Vice Chancellors-Administration and Controllers.

The overall program has been discussed with the Regents Committee on Audit, Chancellors, Executive Vice Chancellors, Vice Chancellors of Administration and Campus Controllers. The Campus Controllers and UCOP Financial Management were given the responsibility for implementing this program.

Formatted: List Paragraph, Indent: Left: 1", Space Before: 10 pt

~~The DA should sign a fiscal close certification letter confirming to the best of the DA's knowledge and belief that the following representations as they relate to both the DA's specific organization at the University location and the nature of the DA's systemwide responsibilities. Accordingly, the following disclosures must be made in writing to the Campus Controller and the Vice Chancellor of Administration: -~~

- I am responsible for the establishment and monitoring of the system of internal control.
- I am responsible for the application of University policies and procedures to ensure the efficient and effective use of resources and to prevent and detect fraud in the areas in which I am involved.
- There are no material transactions or agreements, including the accrual of liabilities that have not been properly recorded in the University's accounting records. In general, items are considered material, regardless of size, if they involve an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the omission or misstatement.
- Communications from regulatory agencies, donors, or other entities concerning noncompliance with laws, regulations, applicable guidelines, directives or with an appropriate standard of care have been disclosed in writing to the Associate Vice President – Systemwide Controller.
- All known allegations of fraud or suspected fraud have been disclosed to the appropriate University official or workgroup.
- The areas in which I am involved manage its funds in compliance with laws, regulations, provisions of contract and grant agreements, and donor restrictions that apply to these funds.

B. Financial Accountability

1. Delegation of Responsibility

a) Financial Stewardship

University management formally delegates signature responsibility to provide a method to control who may approve financial transactions and to meet the University's financial stewardship responsibilities. University employees who have been delegated

Formatted: List Paragraph, Indent: Left: 1", Space Before: 10 pt

Commented [JE2]: Should we as a system say we really want to do this for all DA's, maintain the records for audit purposes and make sure they are all signed. At the moment it's up to the campus discretion how far down we go Deans, AVC etc. they go, say 600 depts. so 600 pieces of paper being tracked each year. If we had a great system say tied to HR maybe an easy option but have we thought through this practically. Also depending on definition of DA could be 1000's another gold mine for the state auditor once it's in our policy.

RAS – See edits that are taking wording directly from Fiscal Closing Certification Q&A.

Formatted: Bulleted + Level: 1 + Aligned at: 1" + Indent at: 1.25"

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

signature authority should understand the University's financial stewardship philosophy, applicable policies, regulations, rules and laws. University employees delegated signature authority are responsible for the application of University policy and procedures to ensure the efficient and effective use of resources and to prevent and detect fraud in the areas in which they are involved in. The delegation should be reviewed for appropriateness on a regular basis or as necessary.

Stewardship responsibilities encompass total oversight of the resources assigned to each employee as well as those resources available for use. Financial stewardship responsibilities include:

- Spending money that reflect the action of a prudent person and monitoring expenditures in a way that the members of the general public would expect.
- Purchasing goods and services in the most efficient and cost effective manner possible and in accordance with University purchasing policies.
- Helping others in their financial stewardship efforts.
- Being accountable for your actions, equipment, funding and time.
- Encouraging others to be good stewards of University resources.

b) Accountability Structure

Each department dean or manager and DA shall be responsible for developing an accountability structure that adheres to the following principles:

- Reporting lines and communication channels must be clear to enable accountability.
- Accountability cannot be delegated.
- A person cannot delegate greater responsibility than he or she possesses.
- Tasks shall only be delegated to people who are qualified to perform them. A qualified person must:
 - be actively involved in the tasks being performed;

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

- have the appropriate knowledge and technical skills to perform those tasks, including knowledge of relevant regulations and policies;
- understand the key control role the person plays in performing the task; and
- have the authority to carry out the tasks.
- A person delegating tasks is responsible for ensuring that those tasks are being properly performed.
- ~~The DA must keep a complete, up-to-date record of the delegations, as well as an audit trail of modifications to them. The DA must verify that delegations are appropriately decided and communicated, documented, and periodically reviewed for accuracy, completeness and effectiveness.~~
- The DA must designate ~~an~~ individuals with responsibility for updating the location's administrative computer security system to grant department employees access to prepare, review, or inquire against on-line systems.

Commented [JE3]: Theory is good but practical side – same comments as before. Plus does this duplicate an earlier section so reader may be confused to keep these records centrally but also the DA must keep them. Maybe only say in one place of policy.

AH – Delete this bullet point.

Commented [JE4]: Maybe sort of old school in some areas, We could have each manager authorizing on line system access system by system decided centrally. People don't always fill in a form to somebody who then grants system access updates, sometimes direct to the system with no human intervention and also potentially more paper work in documenting this for the DA .

RAS– stet: Won't that be already part of change control procedures anyway?

2. Preparing and Reviewing Financial Transactions

Two people ~~will be~~ required to process each financial transaction. The first person (Preparer) enters information about the transaction, and the second person (Reviewer) reviews each financial transaction to ensure that the Preparer has properly fulfilled his or her function. Both a Preparer and Reviewer must be involved in each financial transaction, and the Preparer and Reviewer ~~should can~~ not be the same individual.

Commented [JE5]: Seems very prescriptive, Doesn't cover low value self-approved transactions, not that clear on potential post review processes. The tone of the way it's written seems more around the old methods of always somebody processes the individual transaction and somebody then approves that individual transaction.

RAS - I think this is sufficient for a high level policy. Specific \$ thresholds and exceptions to this rule can be noted in individual location policies. At a high level, this should be the rule of thumb.

There should be no material transactions or agreements, including the accrual of liabilities that have not been properly recorded in the University's accounting records.

Reviews should be properly documented ~~to show proof of review~~. Please see Section IV for the responsibilities of both the Preparer and the Reviewer.

C. Financial Management

Each operating department requires financial resources in order to perform its role in the University's mission of research, teaching and public service.

1. Safeguarding University Assets

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

University assets must be safeguarded from loss or unauthorized use. Adequate safeguards include the following:

- All cash, checks or cash equivalents collected at major and sub cashiering stations, department/units and all petty cash funds, are processed and managed in compliance with the requirements of [BUS-49](#), *Policy for Cash and Cash Equivalents Received*.
- All department assets are properly described and accounted for in the Financial System. Actual physical assets, as recorded in the equipment inventory system, are compared to assets recorded in the Financial System at least once per year. Discrepancies are resolved in a timely manner, and adjustments to asset records must be documented and approved. (Refer to [BUS-29/Management and Control of University Equipment](#)).
- Access to any forms or on-line systems that can be used to alter financial balances must be restricted to qualified and competent employees who require such access to perform their University duties.

2. Safeguarding Information

Protect personally identifiable information or confidential information obtained in the course of handling financial transactions and data must be safeguarded from unauthorized access and use. Please see [IS-3](#), *Electronic Information Security*, for guidelines on safeguarding personal or confidential information.

VI. RELATED INFORMATION

Accounting Manual Chapters

- [P-196-13](#), Payroll: Attendance, Time Reporting, and Leave Accrual Records
- [P-196-16.5](#), Payroll: Official Pay Dates
- [P-196-21](#), Damage Payments for Services Performed Before Loyalty Oath Is Signed
- [P-196-30](#), Payroll: OASDI and Medicare Contributions
- [P-196-78](#), Payroll: UCRS Accounting Procedures
- T-182-73, Taxes: Sales and Use Tax

Business and Finance Bulletins

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

- [BUS-29](#), Management and Control of University Equipment
- [BUS-43](#), Materiel Management
- [BUS-49](#), Policy for Cash and Cash Equivalents Received
- [G-38](#), Tax Exemption and Refund Claims Filing for Property Leased by the University
- [IS-3](#), Electronic Information Security
- [IS-10](#), Systems Development Standards
- [RMP-1](#), University Records Management Program
- [RMP-2](#), Records Retention and Disposition: Principles, Processes, and Guidelines

[University of California Sales & Use Tax Manual](#)

[University of California Whistleblower Policy](#)

[2 CFR Part 200](#): Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards

VII. FREQUENTLY ASKED QUESTIONS

Not applicable.

VIII. REVISION HISTORY

~~XX/31/20156~~: Codification of UCOP Financial Policy previously posted on the CFO Division website into a new systemwide Business and Finance Bulletin.

Commented [WU6]: Change to include policy creators.



Principles of Accountability with Respect to Financial Transactions

Responsible Officer:	AVP - Systemwide Controller
Responsible Office:	FA - Financial Accounting
Issuance Date:	[Issuance Date]
Effective Date:	[Effective Date]
Last Review Date:	
Scope:	<p>This policy applies to any person working for or conducting business on behalf of the campuses, medical centers, Office of the President, and Agriculture & Natural Resources.</p> <p>This policy does not apply to Lawrence Berkeley National Laboratory (LBNL).</p>

I. POLICY SUMMARY _____ **1**

II. DEFINITIONS _____ **2**

III. POLICY TEXT _____ **2**

IV. COMPLIANCE / RESPONSIBILITIES __ **7**

V. PROCEDURES _____ **9**

VI. RELATED INFORMATION _____ **16**

VII. FREQUENTLY ASKED QUESTIONS __ **16**

VIII. REVISION HISTORY _____ **16**

Contact:	Ruth Satorre
Title:	Director Corporate Accounting
Email:	Ruth.Satorre@ucop.edu
Phone #:	(510) 987-0414

I. POLICY SUMMARY

This policy provides an overview of financial accountability, financial management, data integrity, and compliance associated with financial transactions throughout the

University. Campuses should develop policies and procedures to ensure these financial transaction accountability principles are met.

II. DEFINITIONS

Financial stewardship is defined as the responsibility for managing University resources wisely and executing these responsibilities with integrity and ethical conduct. These resources include time, money, people and property. When University employees manage public resources in an efficient, economical and ethical manner, the result will be better achievement of the University's overall missions of teaching, research and public service. Financial stewardship includes the responsibility for establishing and monitoring the system of internal control.

III. POLICY STATEMENT

A. *Background*

Under [Regents Standing Order 100.4: Duties of the President of the University](#), certain duties are delegated to the President, including the authority to redelegate any of the duties of the office, except service as an ex officio Regent.

The President redelegated certain duties to the campuses such as the authority to execute contracts, agreements and to authorize spending disbursements. For a list of duties redelegated by the President, please see the [delegation authority index](#).

The Chancellors have redelegated certain authority to departments and schools to initiate transactions. This policy outlines the requirements for individuals who have been delegated the authority to process financial transactions.

The dean or manager of each school or department, while responsible for managing the department's financial resources, will normally delegate the overall financial management administration to a Department Administrator (DA).¹ The DA is responsible for developing an appropriate structure for handling the department's financial resources, within the boundaries set by the controller's office, the budget office, procurement and other central units. The DA should determine how to divide or segregate the tasks among different people to reduce the risk of error and inappropriate or fraudulent actions. Segregating the tasks require dividing the responsibility for recording, approving transactions, handling the financial resources and reviewing and reconciling.

These requirements apply to department administrators and to staff at shared services units who process transactions on behalf of departments.

¹ If financial management administration is already delegated to centralized administrative units (*outside* the departments), then the department **should not** delegate its financial resource management unless there is an overriding business need to do so.

B. Financial Management

1. Monitoring and Evaluating Financial Data

Each department head and DA must establish monitoring procedures to provide assurance that financial transactions are accurately recorded and comply with applicable regulations, policies, departmental budget plans, etc.

C. Data Integrity

1. Managing University Data

Financial management decisions affect every aspect of the University, but such decisions can only be as good as the data on which they are based. Consequently, each department—including shared services units—must establish and implement procedures to ensure data integrity. These procedures must be documented and provide reasonable assurance that transactions are valid, supported by proper documentation and recorded in an accurate and timely manner in the University's financial records. Each transaction must be authorized in accordance with University policies and campus practices.

2. Establishing Separation of Duties Controls for Data Integrity

No single individual shall have complete control over all processing functions for any financial transaction. If the number of employees in a department is limited, causing one person to perform multiple functions, the department must assign a second person, with the appropriate knowledge and responsibility level, to review the work for accuracy, completeness and timeliness, or combine these functions with another unit. No single individual is authorized to approve their own transaction; all transactions must be approved by someone other than the individual initiating the transaction.

3. Departmental Computing Responsibilities

If a department is operating a system or application that will handle financial transactions, the department must ensure experienced and well-trained technical professionals are supporting the department's computing needs. Such support can be contracted for or provided by a department itself through the IT department.

If a department is developing or acquiring information systems for their use, the requirements in [IS-10](#), *Systems Development Standards* must be followed.

D. Compliance

Every employee who conducts transactions that affect University funds must understand and comply with all applicable laws, regulations, and special restrictions. To ensure compliance, each department head and DA shall adopt the following practices:

1. California State Oath of Allegiance

Departments will ensure that every University employee signs the *State Oath of Allegiance*, at the date of hire, but no later than the time at which the employee begins providing compensable service. For more information, please see Accounting Manual Chapter [P-196-21](#), *Damage Payments for Services Performed Before Loyalty Oath Is Signed*, and [Campus Procedures and Frequently Asked Questions: Damage Payment for Services Performed before Loyalty Oath is Performed](#).

2. Financial Reporting

Department Staff will record transactions in compliance with applicable financial reporting requirements, including Generally Accepted Accounting Principles (GAAP), Governmental Accounting Standards Board (GASB) Statements, Cost Accounting Standards Board (CASB) Statements, and applicable policies and standards of the University, campuses, and medical centers.

Accounting principles must be applied consistently. Financial Management functions and departments at the campus and system wide levels are entrusted with ensuring consistent, University-wide application of these accounting principles.

Reports to sponsoring entities will be made according to the specific reporting requirements. In general, most sponsoring entities require adherence to GAAP. Additionally, federal agencies and entities which serve as conduits for federal funds require adherence to [2 CFR Part 200](#) - *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*.

3. Records Retention

Each DA will maintain financial records in compliance with regulatory requirements and University policy. In cases where there is pending litigation or audits, records must be maintained until the action is concluded. Financial records may be retained by a shared services unit if the unit is formally identified as the office of record. For more information on records retention, refer to the local records management coordinators, [RMP-1](#), *University Records Management Program*, and [RMP-2](#), *Records Retention and Disposition: Principles, Processes, and Guidelines*.

4. Expenditures

All expenditures must comply with applicable regulatory and legal requirements and University policy.

All expenditures and actions affecting a person's compensation must adhere to applicable regulatory and legal requirements and University policy.

5. Tax Laws and Regulations

To comply with tax regulations, each DA must ensure that appropriate personnel are knowledgeable of the various tax authority requirements applicable to their operations.

For more information, see the [University of California Sales & Use Tax Manual](#) and Accounting Manual Chapter T-182-73, *Taxes: Sales and Use Tax*.

6. Exemption from Property Taxes in California

The University is generally exempt from paying real and personal property taxes in California, as described in [G-38](#), *Tax Exemption and Refund Claims Filing for Property Leased by the University*. When necessary, the Facilities Management Department or other appropriate campus department will file the exemption reports and claims to receive refunds of such taxes paid on leased property for the departments.

7. Reporting Fraudulent or Illegal Acts

Any person who becomes aware of potential fraudulent or illegal business transactions conducted in the name of or against the University shall properly report the potential fraudulent or illegal act to the appropriate University official or workgroup. This includes:

- Any person who suspects that fraud or illegal activities are taking place in his or her department must report that suspicion immediately in accordance with the [University of California Whistleblower Policy](#).
- Individuals conducting business on behalf of the University are personally responsible for the consequences of any violations they commit.
- Individuals conducting business on behalf of the University must do so for the benefit of the University. Where a potential for personal gain exists, this potential conflict of interest must be reported immediately,

and be carefully evaluated before any financial transactions are allowed to occur.

For complete guidance on reporting irregularities, see the [University of California Whistleblower Policy](#).

8. Response to External Audits from Regulatory Agencies

Internal Audit must be immediately notified when the University receives notification of any audit or review by an external regulatory agency. Communications from regulatory agencies, donors, or other entities concerning noncompliance with laws, regulations, applicable guidelines, directives or an appropriate standard of care must be disclosed in writing to the Associate Vice President-Systemwide Controller.

IV. COMPLIANCE / RESPONSIBILITIES

Function	Responsibilities
Associate Vice President-Systemwide Controller	<ul style="list-style-type: none"> • Establish and update the policies set forth in this Bulletin.
Department Heads and Department Administrators (DAs)	<ul style="list-style-type: none"> • Understand all relevant regulatory requirements, the campus system, the University policies, and purpose of each transaction; • Develop an accountability structure; • Ensure department manages financial resources in an efficient and cost-effective manner; • Establish monitoring procedures to provide assurance that financial transactions are appropriate, are accurately recorded and comply with applicable regulations, policies, etc; • Develop procedures to ensure data integrity; • Conduct transactions in compliance with applicable financial reporting requirements; • Maintain financial records in compliance with regulatory requirements and University policy; • Departments that conduct sales activities must charge sales tax and properly account for sales tax collected; • Ensure cash and cash equivalents are secure; • Ensure credit card and bank account information complies with data security handling standards; • Departments making purchases must include a provision for sales and use taxes when making orders; • Departments paying individuals must ensure appropriate income tax reporting, including contractors, non-resident aliens, 1099 reportable income, relocation, etc.; • Submit accurate and timely data to Campus Payroll Office, UC PATH and/or other appropriate department; • Have experienced and well-trained technical professionals to support the department's computing needs.
Shared Services Unit	<ul style="list-style-type: none"> • Understand all relevant regulatory requirements, the campus system, the University policies, and purpose of each transaction; • Develop an accountability structure;

University of California – Policy [Policy Number]
Principles of Accountability with Respect to Financial Transactions

Function	Responsibilities
	<ul style="list-style-type: none"> • Ensure appropriate documentation is provided that provides assurance that financial transactions are appropriate, • Ensure transactions are accurately recorded and comply with applicable regulations, policies, etc; • Develop procedures to ensure data integrity; • Conduct transactions in compliance with applicable financial reporting requirements; • Maintain financial records in compliance with regulatory requirements and University policy; • Sales activities must charge sales tax and properly account for sales tax collected; • Purchases must include a provision for sales and use taxes when making orders; • Have experienced and well-trained technical professionals to support the department’s computing needs.
Preparer	<ul style="list-style-type: none"> • Understand all relevant regulatory requirements, the campus systems, the University policies, and the purpose of each transaction; • Enter accurate data into all fields on a transaction document or application system screen; • Record an accurate and thorough explanation of each transaction; • Ensure that the proper Full Accounting Units (FAUs) are entered; • Ensure that any new account and fund linkages requested are appropriate; • Be aware of basic policy, regulatory, and other requirements; • Resolve any questions which come to mind during the completion of the transaction; and • Provide the completed transaction, with any supporting documents, to a Reviewer.
Reviewer	<ul style="list-style-type: none"> • Review all transactions within a reasonable time; • Inspect each transaction to ensure the Preparer properly fulfilled his or her responsibilities; • Ensure that each transaction complies with policy, regulatory, and other requirements; • Resolve all questions that arise concerning a transaction, or ensure the transaction is reversed until the questions are resolved; • Notify the DA if he or she will be absent from work, so another Reviewer can be assigned; and • Notify the DA when he or she is returning to work from an absence.
Chief Procurement Officer, Authorized Buyers, or Specified University Staff	<ul style="list-style-type: none"> • Execute the purchases of: <ul style="list-style-type: none"> ○ Real estate and construction projects; ○ Services of independent consultants; and ○ Legal services.
Departments Engaged in Unrelated Business Income (UBI) Activities	<ul style="list-style-type: none"> • Maintain information supporting whether or not the income is taxable; • Complete UBI questionnaires and worksheets for UBI activities and send them to the appropriate Campus Tax Service Coordinator, who will review and forward them to UCOP Tax Services; and • Account for all taxable UBI earned in an income-producing fund approved by Financial Accounting.
Campus Payroll Office, UC PATH, and/or other	<ul style="list-style-type: none"> • Withhold and remit Federal and State taxes on compensation based upon the individuals’ Form W-4;

Function	Responsibilities
appropriate department	<ul style="list-style-type: none"> • Complete the required quarterly tax returns; • Distribute Forms W-2 to employees; • Report information on non-compensation payments to payees outside the University or University employees on annual reporting forms such as Forms 1099, 1098-T, or 1042-S.
Internal Audit	<ul style="list-style-type: none"> • Be notified when the University receives notification of any audit or review by an external regulatory agency. • The delegation to an External Audit Coordinator depends on the type of external regulatory agency and the type of audit conducted.
Facilities Management Department or the appropriate campus department	<ul style="list-style-type: none"> • File the exemption reports and claims to receive refunds of such taxes paid on leased property for the departments.

V. PROCEDURES

A. *Financial Principles*

All employees with financial transaction authority redelegated to them should adhere to the following:

1. Accountability

Assigning responsibilities and maintaining information on activities so that they are traceable to the specific individual accountable for the transaction or activity.

2. Authorization and approvals

Transactions must be approved by individuals in roles at the appropriate level within the organization and who have been properly granted the appropriate authority.

3. Documentation

Transactions must be supported by documentation and the transactions should comply with University policies.

4. Physical controls over assets

Physically secure assets (equipment, inventories, cash, checks, etc.) should be periodically counted and compared to the assets on record in accordance with UC Policy.

Limit data access to individuals whose duties are aligned with their need to access the data and protect confidential information.

5. Management overrides

Prevent activities to circumvent controls or manipulate transactions, either intentionally or unintentionally.

6. Reconciliations or Ledger Vouching

Ensure the completeness and accuracy of transactions and timely investigation of any discrepancies. Promptly and regularly match transaction data from source systems to destination systems.

7. Supervisory oversight

In conjunction with the fiscal close across all locations, University policy requires a signed “Fiscal Close Certification Letter” from those with fiscal responsibility. The letters are intended to enhance the level of integrity in the financial reporting process by demonstrating due diligence by those with fiscal responsibility. This letter is a component of a broader program to enhance the integrity in the fiscal closing process, ensure disclosures are adequate and provide an avenue for all relevant issues known by campus management to be considered by those responsible for signing the overall campus management representation letter (i.e., the Chancellors, Executive Vice Chancellors, Vice Chancellors-Administration and Controllers).

The overall program has been discussed with the Regents Committee on Audit, Chancellors, Executive Vice Chancellors, Vice Chancellors of Administration and Campus Controllers. The Campus Controllers and UCOP Financial Management were given the responsibility for implementing this program.

Accordingly, the following disclosures must be made in writing by those with fiscal responsibility to the Campus Controller and the Vice Chancellor of Administration as part of the annual fiscal close certification process:

- I am responsible for the establishment and monitoring of the system of the policies, processes and practices of internal control in my department.
- I am responsible for the application of University policies and procedures to ensure the efficient and effective use of resources and to prevent and detect fraud in the areas in which I am involved.
- There are no material transactions or agreements, including the accrual of liabilities that have not been properly recorded in the University’s accounting records. In general, items are considered material, regardless of size, if they involve an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable

person relying on the information would have been changed or influenced by the omission or misstatement.

- Communications from regulatory agencies, contract and grant agencies, or other entities concerning noncompliance with laws, regulations, applicable guidelines, directives or with an appropriate standard of care have been disclosed in writing to the Associate Vice President – Systemwide Controller.
- All known allegations of fraud or suspected fraud have been disclosed to the appropriate University official or workgroup.
- I understand and agree that I am accountable for ensuring that the areas in which I am involved manage its funds in compliance with laws, regulations, provisions of contract and grant agreements, and donor restrictions that apply to these funds.

B. *Financial Accountability*

1. Delegation of Responsibility

a) Financial Stewardship

University management formally delegates signature responsibility to provide a method to control who may approve financial transactions and to meet the University's financial stewardship responsibilities. University employees who have been delegated signature authority should understand the University's financial stewardship philosophy, applicable policies, regulations, rules and laws. University employees delegated signature authority are responsible for the application of University policy and procedures to ensure the efficient and effective use of resources and to prevent and detect fraud in the areas in which they are involved in. The delegation should be reviewed for appropriateness on a regular basis or as necessary.

Stewardship responsibilities encompass total oversight of the resources assigned to each employee as well as those resources available for use. Financial stewardship responsibilities include:

- Spending money that reflect the action of a prudent person and monitoring expenditures in a way that the members of the general public would expect.
- Purchasing goods and services in the most efficient and cost effective manner possible and in accordance with University purchasing policies.

Principles of Accountability with Respect to Financial Transactions

- Helping others in their financial stewardship efforts.
- Being accountable for your actions, equipment, funding and time.
- Encouraging others to be good stewards of University resources.

b) Accountability Structure

Each department dean or manager and DA shall be responsible for developing an accountability structure that adheres to the following principles:

- Reporting lines and communication channels must be clear to enable accountability.
- Accountability cannot be delegated.
- A person cannot delegate greater responsibility than he or she possesses.
- Tasks shall only be delegated to people who are qualified to perform them. A qualified person must:
 - be actively involved in the tasks being performed;
 - have the appropriate knowledge and technical skills to perform those tasks, including knowledge of relevant regulations and policies;
 - understand the key control role the person plays in performing the task; and
 - have the authority to carry out the tasks.
- A person delegating tasks is responsible for ensuring that those tasks are being properly performed.
- The DA must designate individuals with responsibility for updating the location's administrative computer security system to grant department employees access to prepare, review, or inquire against on-line systems.

2. Preparing and Reviewing Financial Transactions

Two people are required to process each financial transaction. The first person (Preparer) enters information about the transaction, and the second person (Reviewer) reviews each financial transaction to ensure that the Preparer has properly fulfilled his or her function and that the

transaction is approved for reporting in the financial system of record. Both a Preparer and Reviewer must be involved in each financial transaction, and the Preparer and Reviewer cannot be the same individual.

There should be no material transactions or agreements, including the accrual of liabilities that have not been properly recorded in the University's accounting records.

Reviews should be properly documented. Please see Section IV for the responsibilities of both the Preparer and the Reviewer.

C. *Financial Management*

Each operating department requires financial resources in order to perform its role in the University's mission of research, teaching and public service.

1. Safeguarding University Assets

University assets must be safeguarded from loss or unauthorized use. Adequate safeguards include the following:

- All cash, checks or cash equivalents, including credit/debit card transactions, collected at major and sub cashiering stations, department/units and all petty cash funds, are processed and managed in compliance with the requirements of [BUS-49](#), *Policy for Cash and Cash Equivalents Received*.
- All department assets are properly described and accounted for in the Financial System. Actual physical assets, as recorded in the equipment inventory system, are compared to assets recorded in the Financial System at least once per year. Discrepancies are resolved in a timely manner, and adjustments to asset records must be documented and approved. (Refer to [BUS-29](#), *Management and Control of University Equipment*).
- Access to any forms or on-line systems that can be used to alter financial balances must be restricted to qualified and competent employees who require such access to perform their University duties.

2. Safeguarding Information

Protect personally identifiable information or confidential information obtained in the course of handling financial transactions and data must be safeguarded from unauthorized access and use. Please see [IS-3](#), *Electronic Information Security*, for guidelines on safeguarding personal or confidential information.

VI. RELATED INFORMATION

Accounting Manual Chapters

- P-196-13, Payroll: Attendance, Time Reporting, and Leave Accrual Records
- P-196-16.5, Payroll: Official Pay Dates
- [P-196-21](#), Damage Payments for Services Performed Before Loyalty Oath Is Signed
- P-196-30, Payroll: OASDI and Medicare Contributions
- P-196-78, Payroll: UCRS Accounting Procedures
- T-182-73, Taxes: Sales and Use Tax

Business and Finance Bulletins

- [BUS-29](#), Management and Control of University Equipment
- [BUS-43](#), Materiel Management
- [BUS-49](#), Policy for Cash and Cash Equivalents Received
- [G-38](#), Tax Exemption and Refund Claims Filing for Property Leased by the University
- [IS-3](#), Electronic Information Security
- [IS-10](#), Systems Development Standards
- [RMP-1](#), University Records Management Program
- [RMP-2](#), Records Retention and Disposition: Principles, Processes, and Guidelines

[University of California Sales & Use Tax Manual](#)

[University of California Whistleblower Policy](#)

[2 CFR Part 200](#): Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards

VII. FREQUENTLY ASKED QUESTIONS

Not applicable.

VIII. REVISION HISTORY

XX/XX/2017: Codification of UCOP Financial Policy previously posted on the CFO Division website into a new systemwide Business and Finance Bulletin.