Chapter 320, Records and Archives
Section 40, Data Administration Policy
Date: 5/16/16
Supersedes: 2/17/2010
Responsible Department: Informational and Educational Technology
Source Document: IS-2, Inventory, Classification, and Release of University Electronic Information

I. Purpose

This policy defines the roles of Data Trustees, Data Stewards and Data Custodians, and sets provisions and standards to protect institutional data.

This policy applies to the use of institutional data within the University. Any requests from the public for institutional data must be treated as public requests under the California Public Records Act (see Section 320-20.

II. Definitions

A. Authorized users—University employees and contractors who have been granted authorization by a Data Trustee to access institutional data.

B. Data Custodians—individuals and departments designated by the Data Trustee with direct physical control over electronic information systems that house institutional data.

C. Data Stewards—individuals designated by the Data Trustee to be responsible for the day-to-day management of institutional data and access to the data.

D. Data Trustees—vice chancellors, vice provosts, deans (or their designees) who collect, generate, extract, or maintain institutional data.

E. Institutional data—data and information stored in administrative computing systems, including transactional data systems, systems containing historical snapshots, and decision support systems. Examples of institutional data include the financial, student, employee sponsored research, and alumni information contained in UC Davis's major administrative computing systems.

III. Policy

A. Timely and appropriate access to institutional data must be provided to those persons with a University business-related need in the performance of their assigned duties.

B. The access of and disclosure or distribution of institutional data in any medium, except as required by an authorized user's assigned duties, is expressly forbidden.

C. Perusal or use of any institutional data for personal interest or advantage or for non-University purposes is prohibited.

D. Violators of access conditions are subject to disciplinary action in accordance with University policies and collective bargaining agreements.

E. The level of protection, including access control, applied to institutional data should correspond to their sensitivity and their criticality to the mission of the university to ensure that the selected security strategies are adequate to the level of risk without being overly restrictive or burdensome.

F. Units extracting, collecting and storing become Data Trustees for that data and are subject to the same responsibilities as defined in this policy.

G. Data access procedures should be transparent and consistent.

IV. Responsibilities

A. Data Trustees

1. Have responsibility for institutional data, access to the data, and for ensuring that institutional data resources are used in ways consistent with the mission of the University.
2. Develop and implement a documented and effective security policy based on a risk assessment and develop appropriate security controls to ensure that the data is properly protected.
3. Recommend policies, and establish procedures and guidelines for campus-wide data administration activities.
4. Define and document procedures by which users may request permission to access institutional data and define criteria under which access would be granted or denied.
5. Designate a Data Steward for institutional data under the Data Trustee's responsibility.

B. Data Stewards

1. Develop and execute plans to implement policy for data in their functional areas.
2. As a group, recommend policies, procedures and guidelines for campuswide data administration activities.
3. As individuals, manage defined segments of the institutional data, including data integrity and management and documentation of operational processes that define when and who can update, add, or delete data.

C. Data Custodians

1. Implement and adhere to the security policy requirements established by the Data Trustees.
2. In close coordination with the Data Stewards, Data Custodians, implement security measures to protect the integrity, availability, and, if appropriate, confidentiality of institutional data resident on information systems under their control.

D. Authorized users

1. Authorized users may access institutional data only in the performance of their assigned duties.
    a. They must respect the confidentiality and privacy of individuals whose records they access and abide by University policies and restrictions with respect to access, use, security, or disclosure of information.
    b. Authorized users must protect the integrity and, if appropriate, confidentiality of institutional data via logical and physical security controls, as specified by policy and user guidelines.
2. Authorized users who develop departmental information systems using institutional data, or store or cache institutional data are responsible for meeting the same security requirements and subject to the same responsibilities as Data Custodians.

V. Small Cell Sizes

1. The University considers tables containing aggregated data entries of fewer than 10 individuals to create a situation where an individual could be personally identified.
2. Data tables and reports containing cell sizes of fewer than 10 individuals should be carefully reviewed before public release to ensure that the individuals are not easily

traceable and create a potential for the invasion of privacy. Data Stewards and Data Custodians are encouraged to consult with the Information Practices Office to determine if their data is appropriate for public release.

3. This cell size limitation applies to external requests.

VI. Further Information

Contact Information for this policy is the Office of the CIO and Vice Provost, IET: vpiet@ucdavis.edu .

Current lists of data trustees, data stewards, and data custodians are available at http://campusdw.ucdavis.edu/contacts.php.

VII. References and Related Policies

A. State of California statutes:

1. California Information Practices Act of 1977, Civil Code Section 1798 et seq.
2. California Penal Code, Section 502, relating to computer crime and other forms of unauthorized access to computers, computer systems, and data.
3. California Public Records Act, Government Code Sections 6250-6270.

B. Federal statutes and regulations:

1. Stored Wire and Electronic Communications and Transactional Records Access, U.S. Code, Title 18, Sections 2701 et seq.
2. Family Educational and Privacy Rights, U.S. Code, Title 20, Section 1232g.
3. Records Maintained on Individuals, U.S. Code, Title 5, Section 552a.

C. UC Electronic Communications Policy.

D. UC Policies Applying to Campus Activities, Organizations, and Students, Section 130.00 et seq., Policies Applying to the Disclosure of Information from Student Records.

E. UC Business & Finance Bulletins:

1. IS-2, Inventory, Classification, and Release of University Electronic Information.
2. IS-3, Electronic Information Security.
3. RMP-1, University Records Management Program.
4. RMP-7, Privacy of and Access to Information Responsibilities.
5. RMP-11, Student Applicant Records.

F. UC Davis Policy & Procedure Manual:

1. Section 260-40, Memorial/Commemorative Funds.
2. Section 310-21, Computer Vulnerability Scanning Policy.
3. Section 310-22, UC Davis Cyber-Safety Program.
4. Section 310-23, Electronic Communications—Allowable Use.
5. Section 310-24, Electronic communications—Privacy and Access.
6. Section 320-10, Records Management Program.
7. Section 320-20, Privacy of and Access to Information.
8. Section 320-21, Privacy and Disclosure of Information from Student Records.
9. Section 320-22, Collection and Confidentiality of Social Security Numbers.