

Executive Summary

Campus Policy on Data Management, Use and Protection

Policy Website:
<http://dataintegration.vcbf.berkeley.edu>

Email: data@berkeley.edu

Phone: Jill Martin, 3-5694

Why We Have This Policy

The confidentiality, accuracy and availability of campus data is of paramount importance to UC Berkeley's educational, research and public service mission. Today, in every area and at every level of the campus enterprise, members of the campus community: faculty, students, staff, and agents or affiliates of the University, are managing or using campus data. Thus, the reliability and security of information is everyone's responsibility.

The campus' goal is to ensure the responsible management of campus data. Data related problems faced by the campus include intentional and unintentional misuse of data; improper sharing of restricted data; accidental loss of data; inability to access data that is essential to one's work; and ongoing threats presented by hackers and identity theft. The Data Management, Use and Protection policy (DMUP) strives to broadly educate campus members on existing laws and policies governing information management, as well as, their specific responsibilities for data resources under their control. It does so by articulating data stewardship roles and the practices necessary to achieve the campus' goal. An individual may perform any or all of these roles depending on their relationship to a specific data resource.

There is a cost to responsibly managing and protecting data. However, implementing the policy will significantly reduce risks, liability and cost associated with the lax or improper management, use or protection data. In addition, all members of the campus community will benefit from increased protection of individual privacy, strengthened security of our physical plant, improved ease and efficiency in the exchange of campus data and reduction of risk and liability, both legal and financial, to the campus, departments and individuals responsible for data stewardship. The full policy can be found at : <http://dataintegration.vcbf.berkeley.edu>.

Important Policy Features:

- Interprets aspects of UC & UCB information management policies and articulates corresponding practices
- Defines data stewardship roles and responsibilities
- Standardizes terms and procedures for optimizing data management and use campuswide
- Establishes a campus governance system for arbitration of disputes involving administrative data

Applicability

The policy applies only to data whose ownership resides with the University (i.e. campus data); however, the practices articulated in the policy are suggested irrespective of ownership. Campus data are all data prepared, supplied, used, or retained by University employees, within the scope of their employment, or by agents or affiliates of the University, under a contractual agreement, except where data is specifically excluded from University ownership by law, policy, or through special overriding ownership provisions, for example scholarly/aesthetic works, course materials, personal works and student works. Campus data may be in any physical form or characteristic, recorded on any form of communication or presentation. Data are not only stored and transmitted in electronic form. Data may be in the form of handwritten notes, paper files or on a variety of electronic resources, fax machines, printers, computers, networks, servers and the applications that run on them.

The policy covers both "unrestricted" and "restricted" data. Large amounts of campus data are classified as unrestricted and there are lesser responsibilities for its proper management and use. Restricted data are data whose access or use are restricted by federal or state law, UC policy, outside agencies (e.g. research sponsors), or as a result of a risk determination by a Data Proprietor. The policy applies additional responsibilities to the management and use of restricted data.

Certain types of data are unique and may be subject to additional protocols. These data types include sponsored research, survey, marketing, and outsourced data. If an individual and/or department have stewardship of such data, they are responsible for complying with federal, state, or outside agency requirements as well as any further requirements contained in this policy.

DMUP was written to complement and further implement existing laws and policies. In the event the DMUP conflicts with federal or state law or University policy, the federal or state law or University policy will take precedence. The policy does not cover requests for data under public access through the California Public Records Act and the Family Education and Privacy Act.

Data Stewardship Roles

DMUP defines campus data stewardship roles. It also establishes the Data Stewardship Council, through the auspices of the e-Berkeley Steering Committee, as the campus authority on the management, use and protection of campus data. The Data Stewardship Council provides applicable policy, education and governance resources to the campus.

Administrative Official: Control unit heads, deans, department chairs, principal investigators, directors, managers, or other high-level employees having ultimate responsibility for the stewardship of campus data, of which they may or may not be the Data Proprietor.

Data Proprietor: The individual(s) or department with primary responsibility for determining the purpose and function of a data resource. For example, the registrar is the Data Proprietor of student information and a principal investigator is the data proprietor of their own original research data.

Data Custodian: An individual(s) or department that functions as the technical partner of a Data Proprietor and is responsible for the implementation of data systems and the technical management of data resources. For example, IS&T is the Data Custodian of human resource data, and the IT administrator of Haas School of Business is the data custodian of all Haas data systems.

Data Integrator: A manager of a data resource that integrates the data of two or more Data Proprietors, one of which may be the Data Integrator themselves. The Office of Planning and Analysis is an example of a data integrator who integrates faculty, student, human resource, and facilities data into the Cal Profiles system.

Data User: A Berkeley employee, or other individual affiliated with UC Berkeley, granted authorization to access or create campus data and who invokes or accesses campus data for the purpose of performing his or her job duties or other functions directly related to their affiliation with UC Berkeley.

Office of Record: The office designated by the campus as having responsibility for responding to formal data requests, meeting reporting requirements, responding to audits, etc., for specific types of data.

System of Record: An application or system formally designated and used to provide official campus information for reporting and other purposes.

Training

DMUP, itself, is a training document and requires that the policy be made readily available to all affected persons. It affirms the importance of additional training for the proper management, use and protection of campus data. It supports Data Proprietors in requiring specific training in order to access and use their data, for example, FERPA training on student data.

Resources

DMUP provides a variety of resources. It contains a compilation of best practices, which members of the campus community are strongly encouraged to emulate. It has an extensive glossary of data related terms, standardizing their use, and it includes links to related federal and state laws, University of California and UC Berkeley policies. In addition, it details an arbitration process for resolving intra-campus administrative data related disputes.

Violations

Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedure, or other relevant regulations or laws; inappropriately modifying or destroying data; inadequately protecting restricted data; or ignoring the explicit requirements of Data Proprietors for the proper management, use, and protection of data resources.

Planned Additions to the Policy (2004-2005)

We will be adding appendices covering the minimum security standards for securing restricted data, and the official list of campus Data Proprietors. Also, guidelines will be offered that assist in DMUP General Implementation, such as checklists for each stewardship role, guidelines for data dictionaries, and model forms (for employee agreement(s) for managing and using restricted data or sharing data with third parties).