

UC Berkeley Library's Policy on Protected Personal Information

Approved by Library Cabinet June 25, 2004

Effective July 1, 2003, a new provision was added to the California Information Practices Act - Civil Code 1798.29, 1798.82. This provision requires any state agency (including the University of California) with computerized data containing protected personal information to disclose any breach of security of a system containing such data to any California resident whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.

Protected Personal Information is defined by in the Civil Code as an individual's first and last name in combination with any of the following.

- social security number,
- driver's license number,
- financial account or credit card number in combination with any password that would permit access to the individual's financial account.

It is the UC Berkeley Library's policy not to collect protected data unless it is deemed necessary in support of Library business. Any collection of this data must be authorized in writing by the University Librarian.

An example of a library business need to collect this information would be to identify a person borrowing library materials (assuming there is no better means to establish this identification).

If the protected data is collected, it is vital for it to have a written articulated disposition schedule that is strictly followed. Protected data is never allowed to be stored on any library server, desktop, laptop computer, or PDA that is connected to a computer network. Protected data in paper format must be secured in a locked drawer or file cabinet. Exceptions to the above must be included in the written approval of the University Librarian.

If a breach is suspected on a computing system that contains or has network access to unencrypted protected data, the data owner must immediately:

- Remove the computing system from the campus network (e.g., power off the computer, disconnect it from the network jack or wireless network)
- Send e-mail to the Director of the Library Systems Office (LSO) and to the LSO Helpdesk to initiate a analysis of the breach.
- Send e-mail to the AUL or Director in charge of the unit.

For more information on protected information, including links to the Civil Code, see the "Berkeley Campus Plan Implementing the UC Requirements for Protection of Computerized Personal Information" at:

<http://socrates.berkeley.edu:7015/protected.data.html#gq-1>