UNIVERSITY OF CALIFORNIA
OFFICE OF LOAN PROGRAMS
SECURITY AND PRIVACY PROCEDURES

The University of California (UC) is subject to the Gramm-Leach-Bliley (GLB) Act that requires financial institutions to maintain the security and confidentiality of personal information including name, address, phone number, bank and credit card numbers, income and credit history and Social Security numbers.

The Director - Office of Loan Programs and the Manager - Loan Servicing are the designated employees within the Office of Loan Programs (OLP) who are responsible for coordinating the safeguards. The Vice President – Chief Information Officer (VP – CIO), based at the UC Office of the President, serves as the Information Security Program Coordinator for the UC system. The University's Information Security Program is located at http://www.ucop.edu/information-technology-services/policies/ucop-it-policies-and-guidelines/ucop-electronic-information-security-policy.html

Information Safeguarding Risk Assessment

In compliance with the Gramm-Leach-Bliley Act and UC's Information Security Program, OLP completed a risk assessment of all OLP procedures, focusing on the controls over security of protected information collected in the course of originating and servicing loans under the University Housing Programs. A matrix was developed that identifies and analyzes areas of risk for each OLP process. Existing controls were reviewed, and an analysis was completed to determine whether the current controls were adequate. In those cases where the controls were not adequate, action was taken to develop new procedures, update procedural manuals, and implement adequate controls. The matrix is reviewed annually to determine whether any procedural updates are needed.

Employee Training and Management

All of the positions within OLP have been designated as critical positions. As such, all new employees undergo background checks and hiring offers are made subject to completion of the background check.

All employees are trained in the following areas:

- Identifying sensitive information
- Responding to requests for information
- Procedures for locking up paper files each night that contain sensitive information (includes loan files at individual employee desks, as well as locking up file drawers and dense file storage units that hold billing and loan files)
- Procedures for using the keyboard lock functions when away from the computer, including automatic locking after predetermined period of non-use
- Using appropriate passwords and keeping passwords confidential
- Shredding copies of documents that contain sensitive information, rather than disposing of them in the trash
- Reporting suspicious requests for customer information

Critical Information Systems and Storage media

OLP has several databases that contain sensitive data. Those databases are:

Loan Origination software

Loan Servicing software

Imaged records of Loan Files

1098 & 1099 statements

The following safeguards are in effect to ensure this data is secure:

- Access to electronic databases requires a password. Separate passwords are required to access the network, Loan Origination software and Loan Servicing software.

- The OLP computer file server has a firewall to protect the data. No dial-in access to the server is allowed. The computer file server is located in a dedicated secure server room requiring key card access. Access to the secure room is limited to employees with security authorization.

- Computer workstations are locked when staff members are away from their desks.

- Backup CD's containing imaged copies of the loan files and backups of the computer systems are kept in a locked fire file in a key-coded locked room. Access to the locked room is limited to designated employees. Each CD is password protected.

- No sensitive information is transmitted via e-mail

- The on-line loan application on the Apply-Online website is encrypted prior to transmitting the data.

Additional Procedures for protecting sensitive data

- Procedures are in place for records management, retention and destruction
- Procedures are in place for securing desk and confidential-area keys

Detecting, Preventing & Responding to a Breach of Security

A breach of security occurs when unauthorized access to a database or platform occurs or is reasonably believed to have occurred, and which would have offered the perpetrator an opportunity to acquire sensitive personal identity information in a form that is not encrypted. If sensitive personal identity information in the database is encrypted, a breach would occur only if an access method was used, or is reasonably believed to have been used, that would have resulted in decryption.

In the event of a breach or suspected breach of security, the Director of Information Security must be notified. Determination of whether a breach has occurred and what action needs to be taken to notify borrowers of the breach is under purview of the Director of Information Security.