Hope LoanPort

HLP 2014 User Guidelines

Required Security Standards for Participant

1. The ("Participant") shall ensure that its employees and all other third parties that could, as a result of its relationship with the Participant, have access to homeowners' confidential personal non-public financial information ("CPI"), are familiar with relevant federal, state and local laws concerning privacy and confidentiality of homeowners' CPI, and are trained in techniques to ensure that the security of CPI is maintained.

2. The Participant shall appoint one individual as information security manager who shall coordinate compliance with the Participant's information security programs.

3. The Participant agrees to retain as HLP system users ("Users") and employees that have access to homeowners' CPI only those individuals that have demonstrated honesty and integrity in the conduct of their business and personal lives.

4. The Participant agrees to adopt and comply with the National Industry Code of Ethics and Conduct for Homeownership Professionals ("Industry Code").

5. The Participant agrees that it will protect the homeowners' CPI from unauthorized access by complying with industry standards for protecting CPI, and with the following rules and standards, all of which shall be subjects of employee training:

a. Only those who have a legitimate business reason to access a homeowner's CPI may access that information;

b. Once accessed, that information will be used solely for business reasons and shall not be publicized or disclosed to any third party that does not have a reason to access the information;

c. When the business reason for access to the CPI is terminated, the access will be terminated and the Participant will ensure that all CPI in its possession or control is destroyed;

d. All files and other paper documents containing CPI shall be kept in file cabinets, rooms or drawers that are locked each night; Only authorized employees know combinations and the location of keys; No paper documents containing CPI maybe removed from the Participant premises; Facsimiles and surface mail shall be read only by those to whom they are addressed.

e. Access to CPI though the Participant's computer system is limited to those employees and third parties who have a business reason to access such information; Each employee is assigned a unique user name and password for access to the computer system, and databases that contain CPI are accessible only to those with such user names and passwords; Robust security systems on the computers will block unauthorized access to the CPI; Firewalls are installed that will prevent one User from accessing CPI of a homeowner that is the client of another Participant or

User; the Participant will utilize the most recent security systems and thinking in maintaining the security of its computer systems.

f. CPI that is placed on the HLP system for use in the web portal shall not be returned to Participant personnel once it is placed on the HLP system and transmitted through the web portal to the servicers.

g. Employees and Users that violate these rules shall be subject to discipline up to and including dismissal from the Participant.

h. Upon termination of employment, all employees and Users shall return any data in their possession or control, as well as all keys or other access devices, and Participant shall immediately deactivate all passwords and access codes of the terminated employee or User.

Required Security Standards for Participant's Users

Users will respect borrower's rights to confidential treatment of their personal non-public financial information, and will make robust efforts to ensure that the privacy of such records is not breached in any way.

1. Private information will not be requested from homeowners unless it is required (a) for purposes relating to activities engaged in by the homeowner and Participant separate and distinct from qualifying for a foreclosure alternative application, or (b) for engaging in activities required as a part of the HLP system.

2. Users may not disclose a homeowner's personal non-public financial information unless specifically permitted to do so by written consent of from the homeowner.

3. Users may not discuss a homeowner's information, or the fact a homeowner is a client, other than in the work setting, and then only with individuals who have a right to access that information.

4. Users will protect the confidentiality of a homeowner's written and electronic records, and shall store such records only in secure locations; Users will not leave a homeowner's records unattended at any time, and will place such records only in locked cabinets at the end of each work period.

5. Users shall ensure that all computers and other electronic devices such as telephones, facsimile machines, telephone answering machines, email, and other devices on which a homeowner's records are transmitted, located, or stored are password protected if passwords are available to that technology, and the password shall not be made available to any third party.

6. Information will not remain in control of Users longer than is necessary for Users to complete their counseling of the homeowner, and Users will dispose of homeowners' records in a manner

that protects homeowners' confidentiality and complies with all state and federal requirements governing disposal of confidential homeowner records.

7. Users will be familiar with federal and state and local laws relating to privacy and confidentiality and shall be prepared to demonstrate that familiarity.