Overview of National Registry Policy

Appraisal Subcommittee (ASC) Policy Statements 3, *National Registry of Appraisers (Appraiser Registry),* and Policy Statement 9, *National Registry of AMCs (AMC Registry)*, require States that access the full database of Appraiser or AMC Registries adopt and implement a written National Registry database access policy that must include, at a minimum:

1. Designation of Authorized Registry Officials (ARO) with the authority to request Registry access for staff members.

2. The ARO must ensure the list of designated users for the Registries is accurate and that the ASC is notified as soon as practicable of any changes to the designated users such as termination of access privileges, changes to access levels, etc. Requests for additional users must be made by the ARO in writing and identify name and contact information along with the level of access requested.

3. Safeguarding of passwords and other user identification, including a prohibition on sharing logon information.

4. Appropriate restrictions on hardware and use of virus protection software including requirements that all users log off the Registries at the end of each workday and lockouts occur during reasonable periods of absence.

5. Recording of data adequate to demonstrate compliance with all elements of the State's policy and maintenance of those records.

Below is a sample of a State National Registry policy which would be acceptable to the ASC. States are responsible for ensuring the integrity of their access to the Registries. Failure to ensure that integrity, consistent with the requirements of Policy Statements 3 and 9, may result in a denial of access to the Registries.

Sample National Registry Access Policy

The Appraisal Subcommittee (ASC) of the FFIEC has issued Policy Statement 3, *National Registry of Appraisers (Appraiser Registry) and Policy Statement 9, National Registry of AMCs (AMC Registry),* which require that States that access the username and password protected sections of the ASC website have a written policy governing access to the Registries. The [STATE REGULATORY ENTITY] adopts this policy as required by the ASC.

The [STATE REGULATORY ENTITY] appoints [INSERT NAME, TITLE, EMAIL ADDRESS AND TELEPHONE NUMBER] as the Authorized Registry Official (ARO) and will notify the ASC in writing of this appointment. [Restrictions on the ARO's authority are

[INSERT ANY RESTRICTIONS]]. The level of access to be granted is [INSERT LEVEL OF ACCESS TO REGISTRIES].

The ARO must ensure that the list of designated users for the Registries is up to date, accurate, and that the ASC is notified as soon as practicable of any changes to the designated users such as termination of access privileges, changes to access levels, etc. Requests for additional users must be made by the ARO in writing and identify the name and contact information along with the level of access requested. All records related to access to the Registries will be maintained for [INSERT NUMBER OF] years.

The ARO must ensure all users of the Registries understand the following:

1. Username and password security. Users may not share passwords or usernames with anyone, including other associates, management personnel or technical personnel. Passwords are not to be written, displayed or stored where another person may access them.
2. Access security. Users may not log on to the Registries with any other user's identification or otherwise have unauthorized access to the Registries. All users must log off the Registries at the end of each workday, and prior to any extended absence during the workday. As an alternative to logging off the Registries during the workday, users may lock all equipment used to access the Registries if a password is required to unlock the equipment. This option must be verified by technical personnel and records of this verification maintained.
3. Software security. All equipment used to access the Registry must have adequate anti-virus software installed. Technical personnel will verify installation of anti-virus software and ensure that such software is kept current. Written records of verifications and updates must be maintained.

Users of the Registries are responsible for all access made with their username and password. Unauthorized access to Registry data may result in violations of State and Federal laws and expose the State to civil penalties. Unauthorized access or failure to comply with the requirements of this Policy may constitute grounds for disciplinary action and/or termination. The ARO must immediately notify the ASC and the [STATE REGULATORY ENTITY] of any known or suspected breach of security involving the Registry or its data and provide a description of the known or suspected breach.