COMMUNITY PARTNERS for AFFORDABLE HOUSING

Main Office
800 S. Milwaukee Ave., Suite 201
Libertyville, IL 60048

Highland Park Office
400 Central Ave., Suite 111
Highland Park, IL 60035

PRIVACY POLICY

Community Partners for Affordable Housing (CPAH) is committed to protecting the privacy of its Clients participating in all programs. This commitment includes implementing measures and practices that:

- Ensure the security and confidentiality of all Client Information that CPAH may receive in the process of providing services, whether from the Client directly or a third party.
- Protect against any anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to Clients.
- Provide notice to Clients in the event a breach in the security protecting the information occurs.
- Ensure proper disposal of Client information.

A. DEFINITIONS

"*Client Information*" is defined as any record containing nonpublic, personally identifiable information, whether in paper or electronic form, that CPAH obtains from a client or other third party in the process of providing services.

"*Non-Record Material*" shall mean (i) material not filed as evidence of administrative activity or for the informational content thereof; (ii) extra copies of documents preserved only for convenience of reference; (iii) stocks of printed or reproduced documents kept for supply purposes, where file copies have been retained for record purposes; (iv) books, periodicals, newspapers, posters, and other library and museum materials made or acquired and preserved solely for reference or exhibition purposes; and (v) private materials neither made nor received by CPAH pursuant to state law or in connection with the transaction of CPAH's business. Duplicate files, copies, library materials, and stocks of obsolete blank forms or pamphlets originally intended for distribution are not considered to be official records or record copies.

"*Records*" mean all books, papers, maps, photographs, or other official documentary materials, regardless of physical form or characteristics, made, produced, executed, or received by CPAH in connection with the transaction of business and must be preserved as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities.

"*Record Retention Policy*" means CPAH's record retention policy that provides guidance in establishing and maintaining an efficient records management program.

"*Service Providers*" mean all third parties who, in the ordinary course of the CPAH's business, are provided access to Client Information.

B. THE INFORMATION SECURITY POLICY

The five elements of this Policy require CPAH to: (i) designate one or more employees to coordinate this Policy, (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Client Information, (iii) ensure that safeguards are employed to control the identified risks and that the effectiveness of these safeguards is regularly tested and monitored, (iv) select Service Providers that are capable of maintaining appropriate safeguards and require them to implement and maintain such safeguards and (v) evaluate and adjust this Policy based on the results of the testing and monitoring, any material changes to operations, or any other circumstances that have or may have a material impact on this Policy.

1. Safeguard Program Coordinator

CPAH hereby designates Robert Anthony as the person who will be responsible for implementing and maintaining this Policy (the "Safeguard Program Coordinator"). The responsibilities of the Safeguard Program Coordinator include, but are not limited to, the following:

(i) The Safeguard Program Coordinator must identify the individuals at CPAH's office who have access to Client Information and the Safeguard Program Coordinator must maintain a current listing of these individuals.

(ii) The Safeguard Program Coordinator must identify potential and actual risks to the security and privacy of Client Information, evaluate the effectiveness of current safeguards for controlling these risks, design and implement additional required safeguards and regularly monitor and test the application of this Policy.

(iii) The Safeguard Program Coordinator must ensure that (i) adequate training and education programs are developed and provided to all employees with access to Client Information and that (ii) existing policies and procedures that provide for the security of Client Information are reviewed and adequate.

(iv) The Safeguard Program Coordinator must identify Service Providers with access to Client Information, ensure that these Service Providers are included within the scope of this Policy and maintain a current listing of these Service Providers.

2. Risk Identification and Assessment

Under the guidance of the Safeguard Program Coordinator, each employee with access to Client Information must take steps to identify and assess internal and external risks to the security, confidentially and integrity of the Client Information. At a minimum, such risk assessment must consider: (i) employee training and management, (ii) information systems, including network and software design, (iii) information processing, storage, transmission and disposal and (iv) detecting, preventing and responding to attacks, instructions or other systems failures. The Safeguard Program Coordinator must ensure that risk assessments are conducted at least annually and more frequently when needed.

Employee training and management include:

(i) checking references prior to hiring employees who will have access to Client Information;

(ii) asking every new employee to sign an agreement to follow the CPAH's confidentially and security standards for handling Client Information;

(iii) training employees to take basic steps to maintain the security, confidentiality and integrity of Client Information, such as: (a) locking rooms and file cabinets where paper records are kept; (b) using password-activated screensavers; (c) using computer passwords with at least six characters long including numbers; (d) changing computer passwords periodically and not posting passwords near employees' computers; (e) referring calls or other requests for Client Information to the Safeguard Program Coordinator; and (f) recognizing any fraudulent attempt to obtain Client Information and reporting it to the Safeguard Program Coordinator;

(iv) reminding all employees of this Policy and the legal requirements;

(v) limiting access to Client Information to employees who have a business reasons for seeing it; and

(vi) imposing disciplinary measures for any breaches.

3. Client Information Safeguards and Monitoring

The Safeguard Program Coordinator must verify that employees with access to Client Information design and implement reasonable safeguards to control identified risks to the security, confidentiality and integrity of Client Information and that the effectiveness of these safeguards is monitored regularly. Such safeguards and monitoring must include the following:

a. Employee Management and Training

Safeguards for information security include training of those individuals with authorized access to Client Information. The Safeguard Program Coordinator must work develop appropriate training and education programs for all affected current and new employees.

b. Records Safeguards

Safeguards for Records and Non-Record Material containing Client Information must include:

(i) creating and implementing access limitation to Records containing Client Information;

(ii) storing Records containing Client Information in a secure area with limited access;

(iii) protecting Records containing Client Information from physical hazards such as fire or water damage;

(iv) disposing of properly outdated records containing Client Information pursuant to the Secured Destruction of Client Information section of this Policy;

(v) disposing of Non-Record Materials containing Client Information when they cease to be useful pursuant to the Secured Destruction of Client Information section of this Policy; and

(vi) other reasonable measures to secure Records and Non-Record Materials containing Client Information during its life cycle while in CPAH's possession or control.

c. Information Systems Safeguards

"Information Systems" include network and software design, as well as data processing storage, transmission and disposal. CPAH must implement and maintain safeguards to control the risks to Information Systems, as identified through the risk assessment process. Safeguards for the Information Systems must include:

(i) creating and implementing access limitation to Information Systems that stores Client Information;

(ii) using secure, password-protected systems within and outside CPAH for access to the Information Systems that stores Client Information;

(iii) regularly obtaining and installing patches to correct software vulnerabilities;

(iv) permanently removing Client Information from computers, diskettes, magnetic tapes, hard drives or other electronic media prior to disposal;

(v) protecting the Information Systems from physical hazards such as fire or water damage;

(vi) detecting, preventing and responding to network attacks or other Information Systems failures; and

(vii) other reasonable measures to secure the Information System that stores Client Information during its life cycle while in CPAH's possession or control.

4. SERVICE PROVIDERS

The Safeguard Program Coordinator must identify Service Providers with access to Client Information. The Safeguard Program Coordinator must ensure that reasonable steps are taken to select and retain Service Providers that can maintain appropriate safeguards for Client Information and must require Service Providers to implement and maintain such safeguards.

5. MONITORING AND TESTING SAFEGUARDS

The Safeguard Program Coordinator must develop and implement procedures to test and monitor the effectiveness of information security safeguards. Monitoring levels must be appropriate to the probability and potential impact of the risks identified, as well as the sensitivity of the information involved. Monitoring may include sampling, systems checks, systems access reports and any other reasonable measure.

C. NOTICE OF A BREACH TO CLIENTS

Following discovery or notification of a breach of CPAH's security of Client Information, the Safeguard Program Coordinator shall notify Clients at no charge that there has been a breach. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system. The notice may be provided in writing or electronically so long as the electronic notice is consistent with provisions regarding electronic records and signatures for notices legally required to be in writing pursuant to 15 U.S.C. § 7001.

If the Safeguard Program Coordinator notifies more than 1,000 persons of a breach of the security, the Safeguard Program Coordinator shall also notify all Client reporting agencies that compile and maintain files on Clients on nationwide basis, as defined by U.S.C. Sec. 1681a(p), of the timing, distribution and content of the notices. Such notices to the Client reporting agencies will not disclose the names or other personal identifying information of breach notice recipients.

The Safeguard Program Coordinator shall submit a report within five (5) business days of the discovery or notification of a breach of the security of the system data or written material to the Illinois General Assembly. Such report shall include a listing of the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. If the Safeguard Program Coordinator has submitted a report as described in this section, the Safeguard Program Coordinator shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.

D. SECURED DESTRUCTION OF CLIENT INFORMATION

CPAH shall dispose Properly Outdated Records and Non-Record Material containing Client Information in such a manner as to ensure the security and confidentiality of such information. Pursuant to the Disposal Rule, CPAH must take reasonable measures to dispose of Client Information to avoid the unauthorized use of, or access to, Client Information in connection with its disposal.

E. REVIEW AND ADJUSTMENT OF THIS POLICY

The Safeguard Program Coordinator must evaluate and adjust annually this Policy in connection with the results of the testing and monitoring described above, as well as any material changes to CPAH's operations, including changes in technology, the sensitivity of Client Information and any other circumstances that may reasonably impact this Policy. The Safeguard Program Coordinator must review this Policy annually to assure ongoing compliance with GLB Act, the Safeguards Rule, the Disposal Rule, and PIP Act, and as well as consistency with other existing and future laws and regulations.

G. STRICT ADHERENCE TO THE INFORMATION SECURITY POLICY

Employees of CPAH are expected to become familiar with CPAH's policy regarding information security and to strictly adhere to the procedures outlined in this Policy.

By: _____

Printed Name: Robert Anthony

Title: President

EXHIBIT A

CPAH PRIVACY NOTICE

Community Partners for Affordable Housing (CPAH) would like to advise you of its privacy policies. CPAH's services often require the collection of non-public personal information from your application and consumer reporting agencies. This non-public personal information may include your address and other contact information, demographic background, application status, loan status, family income, social security number, employment information, collection and repayment history, and credit history.

We disclose non-public personal information to third parties in these instances: only as necessary to process and service your application, only as necessary to effect, administer or enforce the terms of the services provided to you; with your consent; or as permitted or provided by applicable laws, including the Illinois Freedom of Information Act ("FOIA") and the Privacy Act of 1974. Applicable laws permit disclosure to third parties for certain purposes. Examples of such disclosures include (i) disclosure in connection with enforcement purposes or litigation, audits or other investigations; (ii) to comply with proper requests under FOIA or other federal, state, or other local laws and regulations; and (iii) to federal and state agencies to the extent specifically permitted or required by law.

We do not sell or otherwise make available any information about you to any third parties for marketing purposes.

CPAH protects the security and confidentiality of non-public personal information by limiting and monitoring all physical access to sites where non-public personal information is kept. A complete copy of our written privacy policy is available upon request. If we decide to change our Privacy Policy, we will provide you with a revised privacy policy containing such changes.

If you have any questions, please contact CPAH's President, Robert Anthony, at 847-263-7478.

By: _____

Printed Name: Robert Anthony

Title: President