Northwestern Regional Housing Authority's Privacy and Identity Security Policy

The Northwestern Regional Housing Authority (NRHA) recognizes and respects the privacy expectations of today's consumers, and works diligently to meet the requirements of applicable federal and state privacy and identity security laws and regulations. We believe that making you aware of how we use and protect your non-public personal information ("Personal Information"), and to whom it is disclosed, will form the basis for a relationship of trust between us and the public that we serve. This Privacy and Identity Security Policy provides an explanation of the actions we take with respect to your Personal Information. We reserve the right to change this Policy from time to time consistent with applicable privacy and identity security laws.

The NRHA Board of Trustees has delegated administration of this Policy to the Policy Administrator, who is the NRHA Executive Director or his/her designee. The Policy Administrator will periodically review the procedures and activities that NRHA staff undertake in support of this Policy and will ensure that the Policy remains accurate and effective relative to applicable law and sound business practice. This periodic review will focus on internal information systems, operating procedures, and oversight of monitoring controls.
The Policy Administrator will coordinate staff training, monitor Policy compliance, review reports regarding the detection of any instances of privacy breach or identity theft, and supervise steps taken to resolve such occurrences and prevent future ones. If prompted by these review and compliance activities, the Policy Administrator shall propose changes to the Policy for consideration and action by the NRHA Board of Trustees.

In the course of our business, NRHA may collect Personal Information about you from the following sources:

- from applications or other forms we receive from you or your authorized representative;
- from your transactions with, or from the services being performed by, us, our affiliates, or others;
- from our internet web sites;
- from the public records maintained by governmental entities that we either obtain directly from those entities, or from our affiliates or others; and
- from consumer or other reporting agencies.

Our Policies Regarding the Protection of the Confidentiality and Security of Your Personal Information

We maintain physical, electronic and procedural safeguards to protect your Personal Information from unauthorized access or intrusion. We limit access to the Personal Information only to those employees who need such access in connection with providing products or services to you or for other legitimate business purposes.

Our Policies and Practices Regarding the Sharing of Your Personal Information

We may share your Personal Information with our affiliates such as insurance companies, agents, and other real estate settlement service providers. We also may disclose your Personal Information:

- to agents, brokers, or representatives to provide you with services you have requested;
- to third-party contractors, mortgage lenders, insurance agents, or service providers who provide services on our behalf; and
- to others who provide products or services that we believe you may find of interest

In addition, we will disclose your Personal Information when you direct or give us permission, when we are required by law to do so, or when we suspect fraudulent or criminal activities. We also may disclose your Personal Information when otherwise permitted by applicable privacy laws such as, for example, when disclosure is needed to enforce our rights arising out of any agreement, transaction or relationship with you.

One of the important responsibilities of some of our affiliated companies is to record documents in the public domain. Such documents may contain your Personal Information.

Our Policies and Practices regarding the Security of Your Identity and the Personal Information Related to It

When we receive Personal Information from you in connection with your application for services to be provided by NRHA or by a third party for whom NRHA may be acting as an intake agent, we will take the steps outlined in this Policy to maximize the likelihood that we or the third party will be able to detect, prevent and mitigate identity theft. The Identity Security component of the NRHA Privacy and Identity Security Policy consists of reasonable policies and procedures to:

- Identify relevant indicators, as further described below, that may indicate possible breaches of Identity Security
- Maximize the opportunity to detect those indicators while working with your Personal Information
- Respond appropriately to any detected indicator to prevent and mitigate identity theft;
- Reduce or eliminate potential risks to NRHA and its clients; and
- Ensure the Policy is updated periodically to reflect changes in risks to NRHA clients

I. Identifying Threats to your Identity Security

As NRHA collects and processes your Personal Information, we have identified these Identity Security indicators, set forth within the following categories:

A. Suspicious Documents

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing client personal Information (such as if a person's signature on a check appears forged); and
4. Application for services that appears to have been altered or forged.

B. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the client provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address;
5. Social Security number presented that is the same as one given by another person;
6. An address or phone number presented that is the same as that of another person;
7. An applicant's failure to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers are not required);

8. A person's identifying information is not consistent with the information that is on file for the client.

C. Suspicious Activity or Unusual Use Involving a Client Account

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the client is repeatedly returned as undeliverable;
5. Notice to NRHA that a client is not receiving mail sent by NRHA;
6. Notice to NRHA that an account has unauthorized activity;
7. Breach in NRHA's computer system security; or
8. Unauthorized access to or use of client Personal Information.

D. Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a client or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant: and
4. Indication from a credit report of activity that is inconsistent with a client's or applicant's usual pattern or activity.

E. Alerts from Others

1. Notice to NRHA from a client, identity theft victim, law enforcement official or other person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

II. Detection of Threats to the Security of Your Identity

In its dealings with applicants and clients, NRHA will take the following steps to obtain and verify identities, so as to maximize the chance of detecting the Identity Security threats identified above:

A. New Applicant or Client Accounts

1. Require specific identifying information such as name, date of birth, residential and/or business address, driver's license or other identification as permitted by law or regulation;
2. Verify the applicant's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity, if applicable; and
4. Independently contact the applicant;

B. Existing Client Accounts

1. Verify the identification of Clients if they request information about their program status or their Personal Information, whether in person, via telephone, via facsimile or via e-mail;
2. Verify the validity of requests to change billing addresses;
3. Verify changes in banking or other information given for billing and payment purposes; and
4. Verify addresses when mail NRHA sends is returned as "undeliverable" or otherwise.

III. NRHA Response to Suspected Breach of Identity Security

If an NRHA employee suspects or detects fraudulent activity or if an applicant or client claims to be a victim of identity theft, NRHA will respond to and investigate the situation as set forth below.

A. Fraudulent Activity Detected or Suspected by NRHA employee

The employee should gather all relevant documentation and report the incident to his or her immediate supervisor or to the Policy Administrator. If reported to a supervisor, the supervisor should relay the information to the Policy Administrator.

1. The Policy Administrator will determine whether the activity is fraudulent or authentic.
2. If the Policy Administrator determines that the activity is fraudulent, then NRHA, after determining the level of risk of identity theft to be high, should take immediate action, which may include the following:

    i. Notify the client
    ii. Notify the applicable state or federal law enforcement agency, if appropriate
    iii. Change account information as appropriate
    iv. Not attempt to collect on an account until the Identity Security issue is resolved
    v. Change any online passwords permitting access to accounts
    vi. Refer the client to an appropriate credit risk monitoring entity

B. Fraudulent Activity Detected or Suspected by an Applicant or Client

If an applicant or client claims to be a victim of identity theft, NRHA will make every reasonable effort to follow this procedure:

1. NRHA will encourage the applicant or client to file a police report for identity theft if the individual has not already done so.
2. NRHA will encourage the applicant or client to complete the Identity Then Affidavit developed by the Federal Trade Commission, along with supporting documentation.
3. NRHA will compare the client's documentation with Personal Information in the client's records.
4. Following an investigation, if it appears the applicant or client has been a victim of identity theft, NRHA will consider what further remedial act or notifications may be appropriate under the circumstances.
5. Following an investigation, if it does not appear that the applicant or client has been a victim of identity theft, NRHA will take such action as may be deemed appropriate by the Policy Administrator.

C. General Considerations

In order to maximize the prevention of breaches of identity security, NRHA will strive to take the following general steps to protect applicant or client identify information:

1. Ensure that any elements of the NRHA website that involve transmission of applicant or client data arc reasonably secure.
2. Where appropriate and permitted by applicable law or regulation, ensure complete and secure disposition or destruction of paper documents and computer files containing applicant or client information.
3. Maintain password protection on NRHA computers and set computer screen locks to engage after a set period of time.
4. Keep employee desk and other parts of NRHA offices clear of papers containing applicant or client

information;

5. Maintain up to date virus protection on NRHA computers.
6. Require and keep only that applicant and client information necessary for the operation and administration of NRHA programs.

This Privacy and Identity Security Policy is an important aspect of NRHA's relationship with applicants and clients, and we will strive to maintain a Policy that is consistent with the NRHA mission and with the requirements of applicable law and regulation. Please direct any questions or comments about this Policy to:

E. G. "Ned" Fowler, Executive Director
Northwestern Regional Housing Authority
Post Office Box 2510
Boone, NC 28607

20110221(v2)

NOTICE TO APPLICANTS

This is a notice to you as required by the Right to Financial Privacy Act of 1978 that the Department of Housing and Urban Development and Northwestern Regional Housing Authority have a right to access to financial records held by any financial institution in connection with the consideration or administration of the homeownership or rental funds which may be available to you. Financial records involving your transactions will be available to the Department of Housing and Urban Development, N. C. Housing Finance Agency, financial institutions, insurance companies, and other 3rd party contractors participating in loan or rental transactions without further notice or authorization, but will not be disclosed to another Government agency or Department without your consent except as required by law.

In signing this form you are authorizing Northwestern Regional Housing Authority to request information and verification necessary for the provision of housing benefits and services to your household, and you are acknowledging that you have received, read, understood, and agreed to the attached Northwestern Regional Housing Authority's Privacy and Identity Security Policy. In addition, your signature marks your understanding and agreement with the procedures pertaining to possible breach of Identity Security outlined in the Privacy and Identity Security Policy

_____ _____
Northwestern Regional Housing Authority Applicant Signature/ Date

_____
Applicant Signature/ Date