Privacy and Confidentiality Policy
Handling of Personally Identifiable Information

Policy/Procedure: **Privacy and Confidentiality Policy**
Approved by: **Board of Directors**
Date:

Rebuilding Together Atlanta ("RTA") safeguards the privacy of its clients, donors and employees. All Covered Persons involved in the Use or Disclosure of Confidential (PII) Information through RTA shall be familiar with this Policy and shall comply with this Policy at all times.

I. Purpose

The purpose of this Policy is to ensure that Covered Persons implement RTA's safeguards regarding the protection and privacy of all client and donor data collected, created, received, maintained or disseminated for any purpose by the activities of RTA in the performance of RTA's services, as well as all personal employee information.

II. Scope

This policy applies to all Covered Persons who receive access to client, donor or employee information through RTA. All Covered Persons must at all times respect the privacy of its clients, donors and employees, and not release any personal data relating to such clients, donors or employees.

III. Definitions

"Confidential Information" refers to any data, whether written or oral, that (1) is created or received by or for RTA, and (2) relates to (i) a client's or employee's finances, health or other personal information, and either identifies the client or employee or for which there is a reasonable basis to believe could identify the client or employee, including, without limitation, the client's or employee's telephone number and address or (ii) amounts of contributions made to RTA by its donors.

"Disclosure" means the release or transfer of Confidential Information outside RTA, or permitting access to Confidential Information from outside RTA.

"Covered Persons" means any employee, independent contractor, intern, consultant, officer, director, volunteer or other person who has a reason to know Confidential Information in the course of performing services for or on behalf of RTA.

Personally Identifiable Information (PII). Defined in OMB M-07-16 as "...information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal oridentifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." ***See attached list for non exhaustive list of PII***

Sensitive Personally Identifiable Information (SPII). PII that when lost, compromised or disclosed could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers (credit or debit card numbers).

IV. Requirements

RTA has established the following principles as minimum necessary safeguards to protect the confidentiality of Confidential Information (PII)

1. Confidential Information

A. Covered Persons shall not Use or Disclose Confidential Information to any person, including relatives, friends, and business and professional associates, other than to those persons who have a legitimate need to know such Confidential Information and to whom RTA has authorized such Use or Disclosure. Covered Persons shall Use Confidential Information solely for the purpose of performing services for RTA. This policy is not intended to prevent Disclosure where Disclosure is required by law.

B. Covered Persons must exercise good judgment and care at all times to avoid unauthorized or improper Use or Disclosure of Confidential Information. Conversations in public places, such as restaurants, elevators and public transportation, should be limited to matters that do not pertain to information of a sensitive or confidential nature. In addition, Covered Persons should be sensitive to the risk of inadvertent Disclosure and should for example, refrain from leaving Confidential Information in plain view by the public and refrain from the use of speaker phones to discuss Confidential Information if the conversation could be heard by unauthorized persons.

C. At the end of a director's term in office or upon the termination of a Covered Person's relationship with RTA, he or she shall return or destroy all documents, papers and other materials, regardless of medium, in his or her possession which may contain or be derived from Confidential Information.

2. Confidential Information in Paper Form

A. Covered Persons must ensure that all Confidential Information in paper form is kept confidential and not disclosed.

3. Confidential Information in Oral Form

A. Covered Persons must take reasonable steps to protect the privacy of all verbal exchanges or discussions involving Confidential Information (regardless of where the discussion occurs).

B. It is understood that in certain work environments, Uses or Disclosures that are incidental to an otherwise permitted Use or Disclosure may occur, and such incidental Uses or Disclosures are not considered a violation provided that the Covered Person has met the reasonable safeguards and minimum necessary requirements set forth elsewhere in this Policy.

4. Confidential Information in Electronic Form:

4. Confidential Information in Electronic Form:

Covered Persons must ensure that workstations (including home offices) are equipped with reasonable security measures so that unauthorized persons cannot access Confidential Information on an unattended workstation or through the RTA's server or network. Must restrict access to RTA workstations to personnel who have a legitimate and identified need to have such access, and who have been granted such access in accordance with the RTA's procedures.

Procedures shall be in place to ensure that purged Confidential Information cannot be misused or placed into active operation in RTA without appropriate authorization.

Handling of Personally Identifiable Information (PII)

- Only share or discuss sensitive PII with those who have a need to know for work purposes.
- Do not distribute or release sensitive PII to others outside of RTA until the release is authorized and information redacted
- Before discussing sensitive PII on the telephone, confirm that you are speaking to the right person and inform him/her that the discussion will include sensitive PII. Do not leave messages containing sensitive PII on voicemail.
- Avoid discussing sensitive PII if there are unauthorized persons in the adjacent cubicles, rooms, or hallways who may overhear your conversations.
- Hold meetings in secure spaces (no unauthorized access or eavesdropping possible) if sensitive PII will be discussed.

V. Redaction Requirements

Before Sharing Documents (Internally or Externally)
All documents containing PII must be reviewed and redacted prior to:

Public release
Submission to HUD or partner organizations
Responding to FOIA or Open Records Act requests
Use in training, presentations, or publications

Redaction Methods

Electronic documents: Use redaction tools that permanently remove PII from meta data and visible text.
Paper documents: Use black marker or redaction tape, then scan to confirm data is fully obscured.
Redaction must render PII unrecoverable, not merely hidden or obscure

VI Data Minimization and Retention

Only collect the PII necessary to determine program eligibility and maintain program integrity.
Store PII in secure, access-controlled environments.
Retain documents containing PII according to the RTA Document Retention Policy (typically 5–7 years), then securely destroy (shred or digitally delete) them.

VII Staff Responsibilities

All staff should review the Confidentiality and Handling of PII policy and procedures annually annually.
The Executive Director and Board is responsible for enforcing the policy

Any suspected breach must be reported immediately to the Executive Director and Compliance Officer (Board Treasurer).

Prohibited Practices
Sharing unredacted documents or information via email or unsecured platforms.
Using image overlays (e.g., white boxes) instead of true redaction.
Retaining PII beyond the required retention period without a justified, documented reason.

Compliance
Non-compliance may result in disciplinary actions, up to and including termination of employment or contract.

Policy Review and Updates
This policy will be reviewed annually or upon significant changes to HUD guidance, data protection laws, or organizational operations

Who to Contact with Additional Questions:

The requirements and illustrations listed above are not intended to be complete explanations of RTA's safeguards for protecting the confidentiality of Confidential Information and PII but serve as guidance. . If you have specific questions regarding this Policy, you should contact either RTA's Executive Director or Board Treasurer.

Privacy Act of 1974 (5 U.S.C. 552a)
Title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d
E-Government Act of 2002 (Public Law 107-347)
OMB A-108

Rebuilding Together Atlanta

Sign and return this page to the Executive Director.

Date: _____

I hereby certify that I have received a copy of Rebuilding Together Privacy and Confidentiality Policy.

Signed: _____

2.0 Personally Identifiable Information (PII) Handling Policies and Procedures

2.1 Definition of PII

Per the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Set forth below is a non-exclusive list of information that may constitute PII on its own or in combination with other information:

- Age
- Alias
- Audio recordings
- Biometric identifiers (e.g., fingerprints, iris image)
- Certificates (e.g., birth, death, marriage)
- Credit card number
- Criminal records information
- Date of birth
- Device identifiers (e.g., mobile devices)
- Drivers' License / State ID Number
- Education Records
- Email address
- Employee identification number
- Employment status, history, or information (e.g., title, position)
- Fax number
- Financial information
- Foreign activities
- Full name
- Gender
- Geolocation information
- Home address
- Internet cookies containing PII
- Investigation report or database
- IP / MAC address
- Legal documents or records
- Marital status
- Military status or other information
- Mother's maiden name
- Passport information
- Phone numbers
- Photographic identifiers
- Place of birth
- Protected health information
- Race/ethnicity
- Religion
- Salary
- Sex
- Social security number (SSN)
- Taxpayer ID
- User ID
- Vehicle identifiers
- Web uniform resource locators
- Work address or other business contact information. (HUD does not engage with individuals in an entrepreneurial capacity, but business contact information may still constitute PII because it identifies individuals.)