2250 Eaton Street - Garden Level, Suite B - Denver, CO 80214
(303) 202-6340 - Fax (303) 274-1314
www.Brothersredevelopment.org

PROTECTED INFORMATION POLICY

STATEMENT OF POLICY

It is the policy of Brothers Redevelopment, Inc. (BRI) to protect personally identifiable information of employees and clients. The restrictions and safeguards outlined in this policy provide guidance for employees and contractors that have access to PII retained by BRI to ensure compliance with state and federal regulations.

DEFINITIONS

Personally Identifiable Information (PII) –is any information pertaining to an individual that can be used to distinguish or trace a person's identity. Some information that is considered PII is available in public sources such as public websites, social media profiles, etc.

Public PII includes:

1. First and Last name
2. Address
3. Work telephone number
4. Work e-mail address
5. Home telephone number
6. General educational credentials
7. Photos and video

Protected PII –is defined as any one or more of types of information including, but not limited to:

1. Social security number
2. Username and password or security questions and answers that would permit access to an online account.
3. Passport number
4. Credit card number in combination with any required security code, access code or password that would permit access to the account.
5. Clearances
6. Banking information
7. Biometrics
8. Date and place of birth
9. Mothers maiden name
10. Criminal, medical and financial records
11. Educational transcripts
12. Student, military, or passport identification number.
13. Driver's license number or identification card number.
14. Health insurance identification number.
15. Photos and video including any of the above

Personal information (PI) –means a Colorado resident's first name or first initial **and** last name in combination with any one or more of the following protected data elements that relate to the

resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable.

SAFEGUARDING

PII (i) directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which BRI intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Safeguarding sensitive information is a critical responsibility that must be taken seriously at all times. BRI internal policy specifies the following security policies for the protection of PII and other sensitive data:

- It is the responsibility of the individual user to protect data to which they have access. Users must adhere to rules and agency guidance.
- Users having access to personal information shall respect the confidentiality of such information, and refrain from any conduct that would indicate a careless or negligent attitude toward such information. Employees also shall avoid "office gossip" and should not permit any unauthorized viewing of records contained in a BRI records. Only individuals who have a "need to know" in their official capacity shall have access to such systems of records.

The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. Because BRI employees may have access to personal identifiable information concerning individuals and other sensitive data, we have a special responsibility to protect that information from loss and misuse.

With these responsibilities' employees should:

- Safeguard information at all times.
- Obtain management's written approval prior to taking any sensitive information away from the office. The manager's approval must identify the business necessity for removing such information from the BRI facility.
- When approval is granted to take sensitive information away from the office, the employee must adhere to the security policies described within.

FILES

This section provides guidelines on how to maintain and discard PII. All electronic files that contain Protected PII will reside within a protected information system location. All physical files that contain Protected PII will reside within a locked file cabinet or room when not being actively viewed or modified. PII will also not be sent through any form of insecure electronic communication E.g. unencrypted E-mail or instant messaging systems. Significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded or securely deleted.

REDACTION

Users must redact all, but the last 4 digits of the following kinds of information before filing a document either electronically or on paper:

1. Social security number
2. Passport number
3. Credit card number in combination with any required security code, access code or password that would permit access to the account.
4. Bank account number
5.Date of birth
6. Student, military, or passport identification number.
7. Driver's license number or identification card number.
8. Health insurance identification number.

The easiest and best way to redact a document is to print it, mark through the personal identifiers, and then scan the document to PDF. If you choose to electronically redact a document, please be aware that you may need to take extra steps to ensure that personal identifiers remain redacted.

RECORD DESTRUCTION

See Record Retention Policy. When such paper or electronic documents are no longer needed, BRI shall destroy or arrange for the destruction of such paper and electronic documents within its custody or control that contain personal identifying information (PII) by shredding, erasing, or otherwise modifying the PII making it unreadable or indecipherable through any means.

Moreover, unless BRI agrees to provide its own security protection for the information it discloses to a third party, BRI "shall require" the third-party service provider to implement and maintain reasonable security procedures and practices as appropriate.

BREACH

BRI must report a data breach affecting Colorado residents must notify affected residents and, if more than 500 Colorado residents are affected by the incident, the state's attorney general not later than 30 days after the date of determination that a security breach occurred. Reporting requirements under HIPAA or the Gramm-Leach-Bliley Act still applies. Please notify your manager immediately if you believe there has been a breach. The Manager will notify the Compliance Manager and BRI President.

Revised: July 24, 2018