SEED
SOWING EMPOWERMENT & ECONOMIC DEVELOPMENT, INC.

SOWING EMPOWERMENT AND ECONOMIC DEVELOPMENT INC.

PERSONALLY IDENTIFIABLE INFORMATION POLICY

Application of Policy

Sowing Empowerment and Economic Development Inc. Personally Identifiable Information Policy ("PII Policy") sets forth the standards for Sowing Empowerment and Economic Development Inc. ("SEED") to protect personally identifiable information ("PII"). These standards are cast as practices herein; they represent the set of expectations against which policy compliance will be assessed. Further obligations imposed by law, regulations, contract, or other institutional policies also apply.

All members of the SEED community, including without limitation, staff, employees, volunteers, and contractors, are required to adhere to this PII Policy.

Policy

It is SEED's policy to protect the privacy of personally identifiable information that is within SEED's control. PII is information that can be used to identify an individual, whether on its own or in combination with other personal or identifying information that is linked or linkable to an individual. PII can be that of current and prospective workforce members, students, vendors, visitors, and payors, among others. Privacy requirements regarding minors may require additional consideration regarding information classification and/or handling.

Federal and state information privacy laws require SEED to protect certain elements of PII, often because of the sensitivity of the data and/or its potential for misuse for fraudulent activities or other forms of identity theft. These laws may require SEED to self-report to the state or federal government and/or provide notice to affected individuals if the security of certain PII is breached.

Protection and Handling of PII

The following requirements apply to PII in paper records, electronic records and in oral communications, as well as any aggregation of PII in an electronic format (e.g., databases, webpages, e-mail, spreadsheets, tables, and shared drive).

1. General -- In addition to complying with all applicable legal requirements, SEED further limits the collection, use, disclosure, transmission, storage and/or disposal of PII to that which fulfills SEED's mission.

2. Safeguards -- To protect PII against inappropriate access, use, disclosure, or transmission, SEED requires appropriate administrative, technical, and physical safeguards. Divisional and entity leadership is responsible for documenting security controls and safeguards and risk management consistent with the SEED policy. Examples of physical safeguards include storing documents containing PII in secured cabinets or rooms and ensuring that documents containing PII are not left on desks or in other locations that may be visible to individuals not authorized to access the PII.

3. Collection – Collection of PII should be done in a way that is consonant with the other provisions of this section (e.g., Minimization). Collected data should be appropriate for the intended authorized use, and collection should be conducted according to best practice and legal requirements for the type and purpose of data collected. Since the collection process itself can potentially lead to unintended PII disclosure, considerations of confidentiality in collection and recording should be explicitly addressed.

4. Minimization -- All members of the SEED community (e.g., employees, staff, contractors, and volunteers) are responsible for minimizing the use of PII (including redaction of financial account information, use of less sensitive substitutes such as partial SSN) and minimizing aggregations of PII. The risk of unauthorized disclosure of or access to PII increases with the amount of data. All members of the SEED organization are responsible for ensuring that the number and scope of physical and electronic copies and repositories of PII are kept to the minimum necessary and only for the time where a valid business need for the information exists.

5. Permitted Use within SEED -- Only individuals within SEED who are permitted under law, regulation and SEED policies and have a legitimate "need to know" are authorized to access, use, transmit, handle, or receive PII, and that authorization only extends to the specific PII for which the relevant individual has a legitimate “need to know” for the purposes of performing his or her SEED job duties.

6. Permitted Disclosure to Third Parties -- SEED may release PII to third parties only as permitted by law/regulation and SEED policy. Third party contractors to whom SEED is disclosing PII must be bound by agreements with appropriate PII safeguarding and use provisions.

7. Oral Communications -- Only authorized individuals may engage in oral communications involving PII. Caution is required in all oral communications involving PII, and oral communications involving PII may not take place in any location where the communication may be overheard by an individual not authorized to access the PII.

8. Storage of PII -- PII may be stored only as necessary for the SEED mission and permitted under the SEED policy. Department management is responsible for providing guidelines around where information can be scanned/stored (e.g. in hardcopy, on shared drives, on other media/devices) and how long information may be retained before requiring deletion or

destruction). In addition, divisional and entity leadership is responsible for maintaining an up-to-date inventory of stored or maintained documents, files, databases and data sets containing PII, and their contents and requiring encryption of PII stored on mobile devices, media, or other at-risk devices such as public workstations.

9. Transmission of PII -- PII may not be transmitted to external parties outside SEED (e.g. via mail, fax, e-mail, FTP, instant messaging) without appropriate security controls. Generally, such controls include encryption and authentication of recipients (e.g., password protection of files; verifying fax numbers; cover sheets; marking documents as confidential). Great care is to be taken to ensure that emails are sent only to intended recipients.

10. Disposal -- PII must be destroyed and rendered unreadable prior to disposal. For example, this may include shredding papers or wiping electronic files.

11. Training -- Each SEED department is responsible for ensuring that its personnel complete appropriate training on the SEED information privacy policies and sign confidentiality agreements to the extent necessary and appropriate, before accessing, using, transmitting, handling, or receiving PII.

Enforcement and Exceptions

Each SEED entity and department is responsible for ensuring that its PII handling practices are consistent with the practices described in this PII Policy. This responsibility includes the entire set of activities within *enforcement*, including surveillance and detection of non-compliance with the Policy, the identification and implementation of individual- and organizational-level corrective actions, and (where appropriate) the imposition of sanctions. As a practical matter, it may be occasionally necessary and appropriate to diverge from these best practices to advance the SEED's mission. In such cases, it is the responsibility of the head of the relevant division, entity, or department to ensure that such divergences are approved, documented, and communicated to stakeholders.

Breaches of the Privacy of PII

Known or suspected violations of this policy should be reported promptly. Any incidents that have the potential to damage SEED network operations should be reported immediately. Violators of this policy may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination.