HOOSIER SOCIAL IMPACT FUND INC.
INFORMATION SECURITY PROGRAM

Adopted July 31, 2014

I. Purpose

Hoosier Social Impact Fund Inc. (HSIF) has developed and implemented this Information Security Program (the "Program") to protect critical information, ensure ongoing compliance with applicable laws, and position HSIF for likely future privacy and security regulations. The Program is designed to (i) ensure the security and confidentiality of covered information, (ii) protect against any anticipated threats to the security of such information, and (iii) protect against the unauthorized access or use of such information. The Program incorporates by reference HSIF's policies and procedures that may be required by other applicable laws.

II. Gramm-Leach-Bliley Act (GLBA) Requirements

GLBA mandates that certain firms appoint a designated Program Officer, conduct a risk assessment of likely security and privacy risks, institute a training program for those with access to covered information, oversee third-party service providers and contracts, and periodically evaluate and adjust the Program.

III. Designated Representative

HSIF's Vice President of Communications is designated as the Program Officer responsible for coordinating and overseeing the Program. The Program Officer is responsible for identifying reasonably foreseeable risks to the security, confidentiality, and integrity of customer information; evaluating the effectiveness of safeguards for controlling these risks; designing, implementing, and updating the Program; and regularly monitoring and testing the Program. The Program Officer may designate other HSIF members to oversee and coordinate parts of the Program. Any questions regarding the Program should be directed to the Program Officer.

IV. Scope of Program

The Program applies to any non-public financial information about a person who has a relationship with HSIF that is handled or maintained by or on behalf of HSIF or its affiliates.

For purposes of this policy, the term "non-public financial information" includes customer financial information (in paper or electronic form) required to be protected under the GLBA, and any other financial or credit information that (i) a person provides in order to obtain a financial service from HSIF, (ii) results from any transaction with HSIF involving a financial service, or (iii) HSIF otherwise obtains about a person in connection with providing a financial service to that person, whether or not that information is covered by GLBA.

V. Elements of the Program

A. Risk Identification and Assessment

HSIF will identify and assess internal and external risks to the security, confidentiality, and integrity of non-public financial information that could result in its unauthorized disclosure, misuse, alteration, destruction, or other violation. The Program Officer will establish procedures for identifying and assessing such risks in each relevant area of HSIF's operations, including:

- *Customer Loans:* The Program Officer will coordinate with HSIF members to identify foreseeable risks involved in its provision of financial services, including its loan application and approval processes. This asessment should include risks to the security, confidentiality, and integrity of customer information that could result in its unauthorized disclosure, misuse, alteration, destruction or other compromise.
- *Employee Training and Management*. The Program Officer will coordinate with HSIF members to evaluate the effectiveness of its procedures and practices relating to the access and use of customer financial information. This evaluation will include assessing the effectiveness of HSIF's current policies and procedures, including any policies and procedures related to information collection, storage, usage, and security.
- *Information Systems and Information Processing and Disposal.* The Program Officer will coordinate with HSIF members to assess the risks to non-public financial information associated with HSIF's information systems, including network and software design; information processing; the transmission, storage, and disposal of such information; the use and security of its network; and document retention and destruction. The Program Officer will also monitor potential information security threats and update those systems to deal with known security risks.
- *Detecting, Preventing, and Responding to Attacks*. The Program Officer will coordinate with HSIF members to evaluate network access and security policies and procedures, including those for detecting, preventing, and responding to system attacks or failures. The Officer will also monitor and disseminate information related to known security attacks and other threats to the integrity HSIF's networks.

B. Designing and Implementing Safeguards

HSIF's risk assessment and analysis will apply to all methods of handling or disposing of non-public financial information. The Program Officer will implement safeguards to control the risks identified by these assessments, and regularly test or monitor the safguards' effectiveness.

C. Overseeing Service Providers

The Program Officer will coordinate with HSIF members to raise awareness of, and institute methods for, selecting and retaining only third-party service providers capable of maintaining appropriate safeguards for non-public financial information maintained by HSIF to which the providers will have access. The Program Officer will also work with HSIF members to develop and incorporate standard contract terms with service providers that require them to implement and maintain appropriate safeguards, including but not limited to:

- A specific definition of the confidential information being provided;
- An explicit acknowledgment that the contract allows the provider access to confidential information only for the explicit business purposes of the contract;
- A guarantee that the provider will protect confidential information according to commercially acceptable standards and as rigorously as its own customer information;
- A provision allowing for the return or destruction of all confidential information received by the provider upon completion or termination of the contract;
- A provision allowing auditing of the provider's compliance with the contract terms;

- A provision ensuring that the protective terms survive termination of the contract; and
- A stipulation that any violation of the contract's protective terms is a material breach that entitles HSIF to (1) terminate the contract without penalty, and (2) obtain injunctive relief, without a bond, to prevent or remedy breach of these contract terms.

These standards will apply to all HSIF contracts entered into with third-party providers. The Program Officer must approve any deviation from these standard provisions.

D. Adjustments to Program

The Program Officer is responsible for evaluating and updating the Program based on the risk assessment activities undertaken under the Program, as well as any material changes to HSIF's operations or other circumstances that may have a material impact on the Program.

VI. Approval

HSIF's Vice President of Communications and designated information security officer approved this Information Security Program on July 31, 2014.