IDENTITY THEFT PREVENTION POLICY

emPowerSBC Program

SECTION 1: BACKGROUND

The County of Santa Barbara (the "County") operates a contractual assessment program known as the emPowerSBC program (the "Program") to finance the installation of renewable energy, energy efficiency and water efficiency improvements on private property. The County will not collect or maintain many types of sensitive information in connection with the Program, e.g., social security numbers, driver's license numbers, credit rating information or income information. The County may, however, collect credit card information and certain personally identifying information, e.g., name, address, etc.

SECTION 2: PURPOSE

The County wishes to adopt this Identity Theft Prevention Policy (this "Policy") to help protect Program participants from the loss or misuse of sensitive information and to otherwise establish policies and procedures to detect, prevent and mitigate identity theft in connection with the Program.

This Policy will:

1. Define sensitive information;

2. Describe the physical security of sensitive information when it is printed on paper;

3. Describe the electronic security of sensitive information when stored and distributed;

4. Identify and provide procedures for detecting red flags that are potential indicators of identity theft.

5. Identify the appropriate course of action for responding to red flags; and

6. Provide for the updating of this Policy and administration of our identity theft prevention program.

This Policy was adopted by the Board of Supervisors on _____, 20___.

SECTION 3: SENSITIVE INFORMATION AND ITS HANDLING

A. Definition of Sensitive Information

"Sensitive Information" does not include publicly-available information. The County may collect the following Sensitive Information from Program applicants:

1. Credit card information, including credit card number (in part or whole), credit card expiration date, cardholder name and cardholder address.

2. Employer identification numbers.

3. Certain personally identifying information, such as a Program applicant's date of birth, address, phone numbers and maiden name.

4. For purposes of confirming identity, the last four numbers of a social security number.

B. Handling of Sensitive Information

1. *Hard copies*

Each employee and contractor performing work for the County will comply with the following policies:

a. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

b. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.

c. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.

d. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed or shredded when not in use.

e. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded.

2. *Electronic Copies*

Each employee and contractor performing work for the County will comply with the following policies:

a. Internally, sensitive information may be transmitted using approved County e-mail. All sensitive information must be encrypted when stored in an electronic format.

b. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as the following should be included in the e-mail: "This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

SECTION 4: IDENTITY THEFT PREVENTION PROGRAM

A. Red Flags

The following red flags are potential indicators of identity theft. Any time a red flag, or a situation closely resembling a red flag, is identified, it should be investigated.

1. A participating property owner submits suspicious documents, including documents that appear to have been altered or forged.

2. A participating property owner provides inconsistent or incorrect information.

3. A participating property owner, victim of identity theft, law enforcement agency or other person provides a notice of possible identity theft.

B. Detecting Red Flags

In order to detect red flags, appropriate personnel will verify the identification of participating property owners and certain information that they provide in connection with an application.

C. Responding to Red Flags

1. When a red flag is detected, an employee or contractor must gather all related documentation and investigate the facts, then present this information to the Responsible Official designated below for review.

2. If the Responsible Official determines that there is a reasonable possibility that identity theft has occurred, the Responsible Official must take appropriate action immediately, which may include (i) contacting the participating property owner or (ii) notifying and cooperating with the appropriate law enforcement agency.

SECTION 5: PERIODIC UPDATES TO POLICY

The Responsible Official will periodically review this Policy and will report on an annual basis to the County on any identity theft activity and the agency's response to same in order to evaluate compliance with the Policy, the effectiveness of the Policy and to determine whether the Policy is compliant with applicable law. The Responsible Official will approve changes to the Policy that are necessary to address changing identity theft risks to participating property owners and the safety and soundness of the County.

SECTION 6: PROGRAM ADMINISTRATION

A. Responsible Official

The following employee is the "Responsible Official" who will oversee, develop, implement and administer the identity theft prevention program established by this Policy: The County Executive Officer or his/her designee. The Responsible Official may assign responsibilities for identity theft program implementation to appropriate personnel.

B. Staff Training

Staff training shall be conducted on an annual basis (or as otherwise needed) for all employees and contractors who the County reasonably foresees may come into contact with Sensitive Information or become aware of red flags.

C. Contractor Oversight

The County shall take steps to ensure that the activity of any contractor is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the County engages a contractor to perform an activity in connection with Program.