

**Category:** 100 – GENERAL ADMINISTRATIVE

**Number:** 135

**Subject:** SOCIAL SECURITY NUMBER PRIVACY POLICY

**Purpose:** The Michigan Social Security Number Privacy Act became effective on March 1, 2005. This policy is a result of that Act since it requires that any business or individual who obtains social security numbers during the ordinary course of business is required to create a privacy policy by January 1, 2006.

**Authority:** St. Clair County Board of Commissioner's

**Application:** This policy applies to every department and employee, including elected and appointed officials, of St. Clair County government that obtains a social security number during the course of business.

**Responsibility:** All St. Clair County Department heads, including elected and appointed officials, shall be responsible for the implementation and administration of this policy.

**Policy:** St. Clair County requires all employees, including elected and appointed officials, that obtain social security numbers (or SSN) during the ordinary course of conducting business or supply copies or access to records are to adhere the following rules:

1. Ensure to the extent practicable the confidentiality of the social security numbers;
2. Prohibit unlawful disclosure of the social security numbers;
3. Redact social security numbers from copies of records provided to the public except as otherwise required by law;
4. Limit who has access to information or documents that contain the social security numbers so as to prevent unlawful disclosure;
5. Properly dispose of documents that contain the social security numbers by shredding; and

**Prohibitions on Disclosures of Social Security Numbers:**

Except as authorized or required by state or federal law, court order, or pursuant to legal discovery or process, the MI Social Security Number Privacy Act prohibits the following:

1. Publicly displaying more than 4 sequential digits of an individual's SSN.
2. Using all or more than 4 sequential digits of the SSN as the primary account number for an individual.

3. Visibly printing all or more than four sequential digits of a SSN on any identification card.
4. Requiring an individual use or transmit all or more than 4 sequential digits of his/her SSN over the internet or computer system, **unless** the connection is secure or encrypted.
5. Requiring an individual to use or transmit all or more then 4 sequential digits of his/her SSN to gain access to a website or computer system, **unless** the connection is secure, transmission encrypted or a unique personal ID number is also required.
6. Including all or more then 4 sequential digits of the SSN in or on any document mailed **if** it is visible on or through the packaging.
7. Including all or more then 4 sequential digits of the SSN in any document or information mailed to an individual **unless**:
  - a. State or federal law, rule, regulation, or court order or rule authorized, permits or requires that a SSN appear in the document;
  - b. As part of an application or enrollment process initiated by the individual;
  - c. The document is sent to establish, confirm, or terminate an account, contract, or employee or health insurance benefit, or to confirm the accuracy of a SSN of an individual who has an account, contract, policy, or employee or health insurance benefit;
  - d. The document is mailed at the request of the individual whose SSN appears, or his/her parent or legal guardian;
  - e. The document or information is mailed by a public body under any of the following circumstances:
    1. Document is a public record and is mailed with the FOIA;
    2. Document is a copy of a public record filed or recorded with a county clerk or register of deeds office and is mailed by that office to a person entitled to receive that record; or
    3. Document is a copy of a vital record recorded as provided by law and is mailed to a person entitled to receive that record.
  - f. The document or information is mailed in a manner or for a purpose consistent with the Gramm-Leach-Bailey Act, HIPPA, or section 537 or 539 of the MI Ins Code of 1956
  - g. The document is mailed in the ordinary course of business for administrative purposes to:
    1. Verify a person's identity related to an account, service or employment;
    2. Investigate an individual's claim, credit, criminal or driving history;
    3. Detect or prevent theft or any other crime;
    4. Lawfully pursue or enforce legal rights, such as audit, collection, employee benefit, child or spousal support; or
    5. Provide or administer employee health or retirement benefits, or ownership of shares of stock or other investments;

- h. The use of the SSN is for an administrative purpose in the ordinary course of business, by a person, or a vendor or contractor of a person, to do any of the following:
  1. Verify an individual's identity, identify an individual, or do another similar administrative purpose related to an account, transaction, service, or employment, or proposed account, transaction, service or employment;
  2. Investigate an individual's claim, credit criminal, or driving history;
  3. Detect, prevent or deter identity theft or another crime;
  4. Lawfully pursue or enforce a person's legal rights, including but not limited to, an audit, collection, investigation, or transfer of a tax, employee benefit, debt, claim, receivable, or account or an interest in a receivable or account;
  5. Lawfully investigate, collect, or enforce a child or spousal support obligation or tax liability; or
  6. Provide or administer employee or health insurance or membership benefits, claims or retirement programs or to administer the ownership of shares of stock or other investments.

This Policy and lists of Prohibitions on the Disclosure of the SSN will be distributed to all employees of St. Clair County. All such employee shall comply with this policy and the failure to do so will result in appropriate disciplinary action according its policies. The signed policy will be filed in their personnel file the employee will receive a copy of that signed policy.

**Periodic  
Review:**

The Administrator/Controller shall review this policy and make recommendations for changes as needed.

**Adopted: December 14, 2005**

---

Employee's signature

Date