TREASURER OF STATE'S
PROCEDURES ON PROTECTING PRIVACY

1. PURPOSE

The Treasurer of State takes seriously the protection of personally identifiable information. These procedures provide the requirements for protecting the privacy of people who have personally identifiable information in our databases, electronic and paper files and other records. These procedures cover all Treasurer of State employees. It also covers contractors who gain access to Treasurer of State physical facilities or data or computer systems. These procedures lay out basic handling expectations first for all types of personally identifiable information, and second, it provides important additional handling requirements for sensitive personally identifiable information.

What is "Personally Identifiable Information" and What is "Sensitive Personally Identifiable Information"?

For the purposes of these procedures, "personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

It includes "personal information" as defined by Ohio Revised Code (ORC) 1347.01. Some examples of personally identifiable information are:

- names
- Social Security numbers
- resumes
- correspondence
- addresses
- phone numbers
- driver's license numbers
- state identification numbers
- professional license numbers
- financial account information
- medical and health information
- individuals' job classifications and salary information
- performance evaluations
- employment application forms
- timesheets

"Sensitive personally identifiable information" includes personally identifiable information that the Treasurer of State has discretion not to release under public records law, and it also includes "confidential personal information," which the Treasurer of State is restricted or prohibited from releasing under Ohio's public records law. Examples of "sensitive personally identifiable information" that the Treasurer of State keeps includes:

- Social Security numbers
- a person's financial account numbers and information
- beneficiary information
- tax information
- employee voluntary withholdings
- passwords
- employee home addresses and phone numbers
- security challenge questions and answers
- employees' non-state-issued email addresses
- medical and health information
- driver's license numbers
- confidential personal information (see below)

"Confidential personal information" is personal information that falls within the scope of section 1347.15 of the Revised Code and that the Treasurer of State is prohibited from releasing under Ohio's public records law. It applies to any confidential personal information that is maintained in a paper format or in electronic information system maintained by the Treasurer of State's office.

2. PROCEDURES

The Treasurer of State's employees and contractors must follow these procedures on handling all personally identifiable information and handling sensitive personally identifiable information whenever they know or have reason to know that the information is personally identifiable information or sensitive personally identifiable information.

A. Handling All Personally Identifiable Information

i. Use personally identifiable information only for official, lawful purposes.
ii. Do not access systems with personally identifiable information – whether electronic or paper – if you have not been authorized to do so. Contact your supervisor if you need access.
iii. Enter personally identifiable information accurately. Make a good faith effort to correctly enter data. Never intentionally enter false data.
iv. Take reasonable precautions to protect personally identifiable information from unauthorized modification, destruction, use or disclosure. Follow Treasurer of State information security policies and procedures.
v. Whenever a person requests information that the Treasurer's office maintains about that individual, employees and contractors shall follow the Treasurer's office standard procedures for record requests noting that there is a request to inspect personally identifiable information and proceed accordingly by law.
vi. Only collect personally identifiable information when you have been authorized to do so by the proper TOS manager. Do not create an electronic or paper system of record with personally identifiable information unless you have management's authorization and follow TOS Policy 410 – Confidential Personal Information regarding mandated privacy and security requirements.
vii. Destroy personally identifiable information securely in accordance with TOS records retention schedules and following TOS Policy 105 – Records Retention and the IT Security Policy.

viii. Do not initiate or otherwise contribute to any disciplinary or other punitive action against any individual who reports evidence of unauthorized use of personally identifiable information.

ix. The Treasurer's office monitors its information, systems, other IT assets, employees and contractors for compliance with these procedures. Therefore, employees and contractors have no expectation of privacy when they use state information, systems and IT assets.

B. Handling Sensitive Personally identifiable information

i. **Only access sensitive personally identifiable information for a valid reason directly related to the exercise of the Treasurer of State's power or duty.** Valid reasons include:
   - Responding to a public records request;
   - Administering a constitutional provision or duty;
   - Administering a statutory provision or duty;
   - Administering an administrative rule provision or duty;
   - Complying with any state or federal program requirements;
   - Auditing purposes;
   - Carrying out or assisting with an authorized investigation or law enforcement purposes;
   - Conducting or preparing for administrative hearings;
   - Responding to or preparing for litigation, or complying with a court order or subpoena;
   - Administering human resources, including but not limited to hiring, promotion, demotion, discharge, salary and compensation issues, leave requests and related issues, time card approvals and related issues;
   - Administering an information system;
   - Complying with an executive order or policy; or
   - Complying with a collective bargaining agreement provision.

ii. **Do not access or use sensitive personally identifiable information for any reason other than those listed above.** For example, do NOT access or use sensitive personally identifiable information:
   - for gain or personal profit for yourself or someone else,
   - out of simple curiosity or personal interest,
   - to commit a crime,
   - for retribution, use in a personal conflict, or promotion of a personal point of view, or
   - to harass or embarrass.

iii. **You always have a duty not to disclose sensitive personally identifiable information without proper Treasurer's authorization.** As you do your work, you may inadvertently or unintentionally come in contact with information that you know or have reason to believe is sensitive personally identifiable information. In those circumstances, you have a duty not to disclose that sensitive personally identifiable information to anyone except properly authorized persons.

iv. **If you suspect that sensitive personally identifiable information has been improperly accessed or disclosed, you shall report the incident to your Supervisor, Director, Director of Human Resources, Deputy Treasurer or contact the Treasurer's Data Privacy Point of Contact at (614) 387-2834.**
   - Report quickly and do not disturb evidence.
   - Allow the Treasurer's office management to preserve evidence, eliminate any ongoing risks and make a determination that violations have occurred.
   - To ensure that any investigation is not compromised and that an accurate evaluation of the incident is conducted, only the Director of Human Resources, Deputy Treasurer or the Data Privacy Point of Contact may authorize notifications to affected individuals.
   - Upon a finding that confidential personal information has been accessed for an invalid reason in violation of a confidentiality statute, Revised Code 1347.15, Administrative Code 113-25 or TOS policies, the Director of Human Resources, Deputy Treasurer or the Data Privacy Point of Contact will notify affected individuals.

v. Because confidential personal information (CPI) requires a higher standard of care, employees accessing any CPI maintained at the Treasurer's office, shall follow the privacy procedures in OAC 113-25 and TOS Policy 410.

vi. Nothing in these procedures restrict the release of public records. Personally identifiable information is only sensitive if Ohio law gives the agency discretion on its release. Personal information is only confidential if Ohio law prohibits the agency from its release.

3. Violations

i. Any employee who violates these procedures may be subject to disciplinary action up to and including termination.

ii. Any employee who violates a confidentiality statute, OAC 113-25 or Treasurer's office policies may be subject to criminal charges, civil liability arising out of the employee's actions, employment termination and a lifelong prohibition against working for the State of Ohio.

iii. Any violation of these procedures by a contractor may be considered a material breach of the contract and may subject the contract to termination. Any contractor who violates a confidentiality statute may also be subject to criminal charges and civil liability arising out of the contractor's actions. The vendor may also be subject to vendor debarment.

iv. An employee or contractor who complies in good faith with these procedures is not subject to discipline under these procedures.

v. These procedures do not prohibit an employee from accessing information about himself or herself as long as the person has been granted access to the system and uses authorized processes, or makes a request to the Director of Human Resources

or Data Privacy Point of Contact for a list of the personally identifiable information that the department maintains about himself or herself.

4. Maintenance of These Procedures

These procedures will be reviewed at least once annually to ensure that they remain compliant with Federal and State privacy laws including ORC Section 1347.15, OAC 113-25 and Treasurer's policies.

5. Questions

For questions regarding these procedures, please contact the Treasurer of State's Data Privacy Point of Contact at (614) 387-2834.

6. Revision History

Date	Description
01/02/2013	New Procedure for Protecting Privacy