POLICY ON PROTECTING PRIVACY

POLICY NUMBER: 100-11	EFFECTIVE DATE: 04/23/2012	APPOINTING AUTHORITY APPROVAL:
REPLACES POLICY DATED: New	AUTHORITY: ORC 1347.15 and Rules 123-4-01 through 123-4-05 of the Ohio Administrative Code	

1. PURPOSE

The Department of Administrative Services (DAS) takes seriously the protection of personally identifiable information. This policy provides the requirements for protecting the privacy of people who have personally identifiable information in our databases, electronic and paper files and other records. This policy covers all DAS employees. It also covers contractors who gain access to DAS physical facilities or data or computer systems. This policy lays 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 this policy, "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
- physical characteristics and other biometric information
- tax information
- education information
- individuals' job classifications and salary information
- performance evaluations
- employment application forms
- timesheets

"Sensitive personally identifiable information" includes personally identifiable information that DAS has discretion not to release under public records law, and it also includes "confidential

personal information," which DAS is restricted or prohibited from releasing under Ohio's public records law. Examples of "sensitive personally identifiable information" that DAS 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
- fingerprints and other biometric information
- driver's license numbers
- state ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
- 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 DAS is prohibited from releasing under Ohio's public records law. It applies to Social Security numbers, background check information and job audit information that is maintained in the following five personal information systems only:

- Criminal History Reports for MARCS – Office of Information Technology (paper-based system)
- County Job Audits – Human Resources Division (paper-based system)
- County Lay-Off Records – Human Resources Division (paper-based system)
- County Probation Extension Requests – Human Resources Division (paper-based system)
- County Unclassified Designations – Human Resources Division (paper-based system)

2. POLICY

DAS employees and contractors as outlined above must follow these rules 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 DAS information security policies and procedures.
v. Whenever an individual requests information that DAS maintains about that individual, employees and contractors shall follow DAS Standard Operating Procedure – Request to Inspect Personally Identifiable Information.

vi. Only collect personally identifiable information when you have been authorized to do so by the proper DAS manager. Do not create an electronic or paper system of record with personally identifiable information unless you have DAS authorization and follow DAS - mandated privacy and security requirements.

vii. Destroy personally identifiable information securely in accordance with records retention schedules and following DAS data destruction procedures for particular systems or records.

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. DAS monitors its information, systems, other IT assets, employees and contractors for compliance with this policy. Therefore, employees and contractors have no expectation of privacy when they use state information, systems and IT assets.

B. Handling Sensitive Personal Information

i. **Only access sensitive personally identifiable information for a valid reason directly related to the exercise of a DAS power or duty.** Valid reasons include:
   - Responding to a public records request;
   - Responding to a request from an individual for the list of personally identifiable information the agency maintains on that individual;
   - 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;
   - Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
   - Auditing purposes;
   - Carrying out licensure, permit, eligibility, filing, certifications or other similar processes;
   - 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;
   - Complying with an agency policy or a state administrative policy issued by the Department of Administrative Services, the Office of Budget and Management or other similar state agency; or
   - Complying with a collective bargaining agreement provision.

ii. **Do not access sensitive personally identifiable information for any reason other than those listed above.** For example, do NOT access 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 agency 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 manager or another manager or contact the DAS Data Privacy Point of Contact at (614) 387-1602**.
- Report quickly and do not disturb evidence.
- Allow the DAS response team 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, assistant directors or deputy directors of DAS 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, section 1347.15 of the Revised Code or rules 123-4-01 through 123-4-05 of the Administrative Code, the director, assistant directors or deputy directors of DAS will notify affected individuals.

v. Because confidential personal information (CPI) requires a higher standard of care, employees accessing the following **CPI systems** shall follow the privacy procedure specific to that system:
- See DAS Standard Operating Procedure – Accessing Confidential Personal Information in a Paper-Based System – Criminal History Reports – MARCS.
- See DAS Standard Operating Procedure – Accessing Confidential Personal Information in a Paper-Based System – County Job Audits – Human Resources Division.
- See DAS Standard Operating Procedure – Accessing Confidential Personal Information in a Paper-Based System – County Lay-Off Records – Human Resources Division.
- See DAS Standard Operating Procedure – Accessing Confidential Personal Information in a Paper-Based System – County Probation Extension Requests – Human Resources Division.
- See DAS Standard Operating Procedure – Accessing Confidential Personal Information in a Paper-Based System – County Unclassified Designations – Human Resources Division.

3. Violations

i. Any employee who violates this policy is subject to disciplinary action up to and including termination.

ii. Any employee who violates a confidentiality statute or DAS rules 123-4-01 through 123-4-05 is 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 this policy 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 this policy is not subject to discipline under this policy.

v. This policy does 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 DAS for a list of the personally identifiable information that the department maintains about himself or herself.

4. Maintenance of This Policy

This policy will be reviewed at least once annually to ensure that it remains compliant with Federal and State privacy laws including ORC Section 1347.15 and that it accurately reflects DAS personally identifiable information and systems.

5. Questions

For questions regarding this policy, please contact the DAS Data Privacy Point of Contact at (614) 466-2701.

6. Revision History

Date	Description
04/23/2012	New policy