



TED STRICKLAND
GOVERNOR
STATE OF OHIO

Management Directive
November 20, 2008

Accessing Sensitive Personal Information
Maintained by the State

1. **Protecting the Privacy of Ohioans.** The State of Ohio is dedicated to developing and implementing technology standards that enhance and ensure the privacy and security of Ohio's citizens who have information that is stored in the State's data systems. To that end, this Directive will set forth those procedures that all executive agencies, boards and commissions (collectively, "State Agencies") will implement to ensure that this information will only be accessed to clearly advance a specific, legitimate governmental objective. The policies and procedures outlined in this Directive are in no way intended to constrict the public's access to public records as provided by Ohio law.
2. **The State Can and Should Improve Existing Data Privacy Safeguards.** This Management Directive seeks to develop means of protecting non-public data, by ensuring that agencies have implemented privacy-ensuring strategies that safeguard Ohio citizens' personal information within their control. At a minimum, those safeguards should be based on the following principles:
 - a. No non-public data maintained by any State Agency should be accessed without the use of a password that expires after 180 days;

- b. The director of each State Agency should make an affirmative determination of what employee positions receive a password that authorizes access to non-public information, as well as why access by such employees advances a legitimate business need;
 - c. Each State Agency should have a standard for accessing data based on that agency's ability to articulate that the access is necessary to clearly advance a specific, legitimate governmental objective, and
 - d. Each State Agency should keep a log that details with respect to each access of non-public information:
 - i. Who accessed the information and whether the person who accessed the information was authorized to do so;
 - ii. What information was accessed and for what specific, legitimate governmental objective the information was accessed;
 - iii. When the information was accessed.
3. Definition of "Sensitive Personal Information". As used in this Directive, "sensitive personal information" means non-public personal information that describes anything about a person; that indicates actions done by or to a person; that indicates that a person possesses certain personal characteristics; that contains, and can be retrieved from a system by a name or identifying number assigned to a person; and/or that carries a higher risk to the subjects of the information, if such information is misused or placed in the wrong hands. Examples of "sensitive personal information" may include the following when they are maintained in the State's data systems and are not available under Ohio Public Records Law:
- a. Data related to an individual's educational, financial, health/medical, criminal or employment history;
 - b. Social security numbers;
 - c. Federal tax identification numbers; or
 - d. Financial account numbers.

4. **Establishing Policies Regarding Access to Sensitive Personal Information.** In Executive Order 2007-13S, I ordered all State Agency Directors to designate a Data Privacy Point of Contact (DPPOC), within their respective agency, to work with the State's Chief Privacy Officer in order to ensure that Ohioans' personal data are properly protected. Accordingly, in the State's continuing effort to assure Ohioans that sensitive personal information collected by and provided to the State is handled with the utmost care and regard, I hereby direct the DPPOC for each State Agency to ensure that the following is completed by March 31, 2009:
- a. Documentation of the sensitive personal information maintained by the State Agency, the database(s) in which that information resides and the labeling of information accordingly;
 - b. In consultation with the respective Chief Legal Counsel for the DPPOC's State Agency, or the person acting in that capacity for the agency, the establishment and maintenance of a catalog of laws and administrative regulations and policies, both at the state and federal levels, that govern the storage, use and distribution of sensitive personal information;
 - c. In consultation with the respective Chief Legal Counsel for the DPPOC's State Agency or the person acting in that capacity for the agency, as well as the State's Chief Privacy Officer, establishment of written policies that specifically address when sensitive personal information under the agency's control, may be accessed and how it may be used. Each agency's written policy should include, but not be limited to:
 - i. The identification and/or description of employee positions within each agency that require access to sensitive personal information so that only those who need to, have access to such information;
 - ii. The identification and/or description of the types of sensitive personal information that is properly accessed by particular employee positions;
 - iii. Procedures that ensure that review of sensitive personal information is limited to instances in which access will clearly advance a specific,

legitimate governmental objective. In developing these procedures, non-public sensitive personal information should only be accessed by personnel expressly authorized to do so and only when there is a concrete and articulable reason to believe that personal privacy concerns associated with sensitive personal information are outweighed by the specific, legitimate governmental objective advanced by accessing the sensitive personal information;

- iv. The establishment of prohibitions against using or accessing sensitive personal information for impermissible purposes and the consequences for doing so;
 - v. The establishment of an annual review of the business need and legal basis for collecting sensitive personal information, in an effort to eliminate the necessity of collecting that information whenever possible.
- d. Completion of a Privacy Impact Assessment Form to be developed by the Office of Information Technology and posted on the web by December 1. The Form should assist Agencies in complying with this Directive and should help them assess the risks and effects of collecting, maintaining and disseminating information, as well as privacy protection processes designed to mitigate potential privacy risks.
- e. If a DPPOC is unable to complete the policies outlined in this Directive by March 31, 2009, because of human resource and/or financial constraints caused by Ohio's current budget crisis, then the DPPOC for that agency must report to the director of the Agency by March 31, 2009, the status of the implementation of this Directive, the date by which implementation of the Directive is expected to be completed. Each Agency Director shall be responsible for assuring that this Directive is fully implemented in a timely manner.



Ted Strickland

Ted Strickland, Governor