# DATA ACCESS POLICY

## I. PURPOSE/REASON

To establish departmental requirements for business appropriate uses of the Ohio Secretary of State (SOS) Confidential Personal Information (CPI) stored in SOS maintained computer systems. These expectations are based on federal and state statutory requirements.

On April 6, 2009, Governor Ted Strickland issued the revised Management Directive - "Accessing Confidential Personal Information". This directive sets forth the process that all executive agencies shall follow to implement section 1347.15 of the Ohio Revised Code (ORC). The directive includes a requirement that each state agency develop access policies. The criteria, references, procedures, and requirements are identified in section 1347.15(B) of the ORC.

## II. REFERENCES/ AUTHORITY

**References**

1. Note: ORC references can be accessed at LAWriter's Ohio Revised Code. (http://codes.ohio.gov/) website.ORC 1347.15
2. Ohio Revised Code 1347.01
3. Ohio Revised Code 1347.05
4. Ohio Revised Code 149.43
5. Governors April 6, 2009 Management Directive "Accessing Confidential Personal Information”
6. Public Records and Confidentiality Laws e-manual available on-line
7. Ohio Administrative Code Rule 111-7-02 SOS Employee Access to Confidential Personal Information
8. SOS Information Security Policy
9. Research Policy

**Authority**

This policy is established by order of the Ohio Secretary of State.

## III. SUPERSEDES

Any other previously SOS-issued memorandum, policy, or procedure on this subject.

## IV. SCOPE

This policy applies to all SOS employees, vendors, temporaries, contractors, and consultants.

## V. POLICY

A. Standard

1. The Ohio Secretary of State may need to maintain CPI about Ohio citizens and businesses in order to exercise its mission to provide regulatory protection for oversight of the Elections process, Campaign Finance compliance, custodian of Business Filings, Uniform Commercial Code Transactions (UCC), Document Certification, Historical Records, Ministers Licenses, and Notary Commissions. It is the responsibility of SOS to ensure that this information, whether stored electronically, or on other media, is properly protected.

   This policy establishes the valid reasons for accessing CPI. A threat to the security of CPI represents a threat to the SOS's ability to provide services. Each employee must understand their role in maintaining the security and privacy of CPI they access.

B. Criteria for accessing CPI

1. Each information owner determines the level of access required for an employee of the agency to fulfill his or her job duties. The determination of access to CPI shall be approved by the employee's supervisor, as well as the information owner, prior to providing the employee with access to CPI. Should an employee's job duties change due to a transfer or termination, a review and/or revision to the employee's access to CPI shall be performed. When an employee's job duties no longer require access to CPI, access shall be removed.

C. Reasons for Accessing CPI

1. Access to and use of CPI collected and maintained by the SOS is strictly limited to purposes authorized by SOS. The purpose should be directly related to the system user's official job duties and work assignments.
2. Below are lists of valid and non-valid reasons for accessing CPI (regardless of whether the CPI is maintained electronically or on other media) that are common across all lines of business.
3. Valid Reasons – including, but not limited to:
   a. In the course of administering or performing job duties related to the following processes, authorized employees of the agency would have valid reasons for accessing CPI:

b. Responding to (a) public records requests, when public records are comingled with CPI, or (b) records requests made by the individual for his/her own CPI;

c. Program administration, including (a) compliance with federal/state laws and regulations, (b) processing or payment of filings, (c) eligibility determinations, (d) audits, investigations and oversight, (e) licensing and certification, and (f) administrative hearings;

d. Litigation (including discovery and responding to court orders and subpoenas);

e. Human resource matters (hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);

f. Complying with an Executive Order or policy;

g. Complying with an agency policy or a state administrative policy issued by the Department of Administrative Services (DAS), the Office of Budget and Management (OBM), or other similar state agencies;

h. Research in the maintenance of agency specific programs as allowed by statute;

i. Complying with a collective bargaining agreement provision.
   1. Note that the citations listed above are not all-inclusive. For a more complete list of public records and confidentiality laws applicable to SOS-administered programs, please visit the Public Records and Confidentiality Laws e-manual available online.

4. Non-Valid Reasons - including, but not limited to:
   a. Access that result in personal or political gain.
   b. Commercial use unrelated to official departmental business.

5. Intentional violations of this policy shall result in disciplinary action up to and including removal in accordance with current disciplinary guidelines.

## VI. PROCEDURE

A. Upgrades to existing SOS computer systems, or acquisition of any new computer systems that store, manage, or contain CPI, shall include a mechanism for recording access of CPI by users of the system.

B. Two exceptions for the need to log access to CPI:

1. The access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals. E.g., a helpdesk staff person is requested to assist in the resolution of a program or technical issue and in the course of resolving the issue they must access CPI.
2. The access is for CPI about an individual, and the access occurs as a result of a request by that individual or their legal representative for CPI about that same individual.

C. Information Requests
1. Upon the signed written request of any individual whose CPI may be kept by the agency, the agency shall do all of the following:
2. Verify the identity of the individual;
3. During the pendency of an ongoing investigation about the individual, determine what, if any, records can be shared with that individual;
4. Provide to the individual the CPI that does not relate to an investigation about the individual, or is otherwise not excluded per chapter 1347 of the ORC.

D. Notification of Invalid Access
1. Upon discovery or notification that CPI has been accessed by an agency employee for an invalid reason, the agency shall:
   a. Take steps to notify the person whose information was invalidly accessed as soon as practical, and to the extent known at the time.
2. Delay of Notification
   a. The agency may delay notification for a period of time necessary to ensure that the notification will not delay or impede an investigation or jeopardize homeland or national security.
   b. The agency may delay the notification consistent with measures necessary to determine the scope of the invalid access. This includes which individuals' CPI invalidly was accessed, and to restore the reasonable integrity of the system.
3. Once determined that notification will not delay or impede an investigation, the agency must disclose to the individual the access to CPI made for an invalid purpose.
4. The notification given by the agency shall inform the individual of the type of CPI invalidly accessed, and the date(s) of the invalid access (date approximations shall be as close as possible).
5. Notification may be made by any method determined to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

E. The Secretary of State shall designate an employee of the agency to serve as the Data Privacy Point of Contact, under the working title of Chief Privacy Officer (CPO). The SOS CPO shall work closely with the State of Ohio CPO, and State

Chief Security Officer (CSO), to assist the SOS with the implementation of CPI privacy protections and compliance with Section 1347.15 of the ORC.

F. The SOS CPO will ensure the timely completion of the Privacy Impact Assessment form developed by the State Office of Information Technology (OIT).

G. The CPO will ensure that all SOS computer systems containing CPI employ passwords, or an equivalent form of authentication, as deemed appropriate through a Privacy Impact Assessment to ensure access to CPI is kept secured.

H. All SOS employees shall undergo training that will, at a minimum, include awareness of all applicable statutes, rules, and policies governing access to CPI they may come into contact as part of their assigned job duties.

I. The SOS will create a poster describing agency policies related to the protection of CPI. Copies of the poster will be placed in appropriate locations to ensure visibility by all employees.

J. All agency employees must acknowledge receipt of, understanding of, and compliance with this policy.

K. Discipline

1. Violation of any portion of this policy may result in disciplinary action or contractual penalties and may be cause for termination. Additionally, an employee may be subject to a civil action or criminal prosecution as a result of inappropriate use or misuse of IT equipment.
2. Discipline will be consistent with SOS, civil service and contractual rules and regulations, and the CWA contract. The Ohio Revised Code designates certain misuses of IT equipment as criminal offenses.

## VII. DEFINITIONS

1. "*Access*" as a noun means an opportunity to copy, view, or otherwise perceive. As a verb, "access" means to copy, view, or otherwise perceive.

2. "*Acquisition of a new computer system*" means the purchase of a computer system, as defined in this chapter, which is not a computer system currently in place nor one for which the acquisition process has been started as of the effective date of the agency rule addressing ORC 1347.15 requirements.

3. "*Computer system*" means a "system," as defined by section 1347.01 of the ORC that stores, maintains, or retrieves personal information using electronic data processing equipment.

4. "*Confidential Personal Information* (*CPI*)" means "confidential personal information" as defined in section 1347.15(A) (1) of the ORC. For SOS, CPI includes any non-public information about SOS employees, contractors, and service providers (such as social security numbers and non-work-related addresses).

# DATA ACCESS POLICY

5. "*Employee of the state agency*" means each employee of a state agency regardless of whether he or she holds an elected or appointed office or position within the state agency. "Employee of the state agency" is limited to the specific state agency that has the appointing authority for the employee.

6. "*Incidental contact*" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.

7. "*Individual*", in the context used in ORC 1347.15(C)(1)(b) means the subject of the CPI or the subject of the CPI's authorized representative, legal counsel, legal custodian or legal guardian, and anyone as otherwise permitted under state or federal law acting on behalf of, or in furtherance of, the interests of the subject of the CPI. Individual does NOT include an opposing party in litigation, or the opposing party's legal counsel, or an investigator, auditor or any other party who is not acting on behalf of, or in furtherance of the interests of, the subject of the CPI, even if such individual has obtained a signed release from the subject of the CPI.

8. "*Information owner*" is the one individual appointed in accordance with section 1347.05(A) of the ORC to be directly responsible for a system.

9. "*Person*" means natural person.

10. "*Personal information*" means "personal information" as that term is defined in section 1347.01(E) of the ORC.

11. "*Personal information system*" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the ORC. "System" includes manual and computer systems.

12. "*Research*" means to explore, analyze, or examine data.

13. "*Routine*" means common place, regular, habitual, or ordinary.

14. "*System*" means "system" as defined in section 1347.01(F).

*15. "*Upgrade*"* means a substantial redesign of an existing system for the purpose of providing a substantial amount of new application functionality, or application modifications which would involve substantial administrative or fiscal resources to implement. "Upgrade" does not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements. For the purposes of this policy SOS defines "substantial redesign" to mean any change that modifies greater than 50% of the code in an existing application.

16. "Public Record*" means data that is subject to disclosure through Ohio public records law section 149.43 of the ORC. SOS Information Technology Department (SOS IT)* - SOS IT is responsible for developing, maintaining, and supporting SOS applications. Network and the SOS Helpdesk are responsible for provisioning and de-provisioning functions as they relate to application and data access.

17. *Responsible SOS Program Areas and Program Data Owners* - SOS is charged with administering various programs governed by sections of the Ohio Revised Code (ORC). The Program Area is responsible for authorizing access to specific application(s) and/or data. The Program Data Owner is accountable for granting and revoking access to specific application(s) and/or data. The Program Data Owner is held accountable for the data.

## VIII. ASSISTANCE

For additional information or clarification regarding this policy/procedure, please contact the Human Resources Division.