111-1-02 **Confidential personal information ~~systems~~.**

~~The secretary of state herein establishes a rule for the protection of confidential personal information. Secretary of state systems maintained in the regular course of business that contain personal information that is confidential in nature will be accessed in accordance with this rule established pursuant to division (B) of section 1347.15 of the Revised Code.~~

(A) ~~Definitions~~As used in this rule:~~.~~

(1) "Access" as a noun means an instance of copying, viewing, conveying, or otherwise perceiving, whereas "access" as a verb means to copy, view, convey, transfer or otherwise perceive.

(2) "Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not ~~a computer system~~ currently in place ~~nor one for which the acquisition process has been initiated as of the effective date of the agency rule addressing requirements in section 1347.15 of the Revised Code~~.

(3) "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, processes or retrieves personal information using electronic data processing equipment.

(4) "Confidential personal information" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code ~~and identified by rules promulgated by the secretary of state in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes or administrative rules that make personal information maintained by the secretary of state confidential~~.

(5) "Employee of the secretary of state" means each employee of the secretary of state regardless of whether he/she holds an elected or appointed office or position within the state agency

(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" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

(8) "Information owner" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.

(9) "Person" means a natural person.

(10) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.

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

(12) "Research" means a methodical investigation into a subject.

(13) "Routine" means commonplace, regular, habitual, or ordinary.

~~(14) "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person" as that phrase is used in division (F) of section 1347.01 of the Revised Code means personal information relating to employees and maintained by the secretary of state for internal administrative and human resource purposes.~~

~~(15)~~(14) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.

~~(16)~~(15) "Upgrade" means a substantial redesign of an existing computer system for the purpose of providing a substantial amount of new application functionality, or application modifications that would involve substantial administrative or fiscal resources to implement, but would not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements.

(B) ~~Procedures for accessing CPI.~~

~~For personal information systems, whether manual or computer systems, that contain confidential personal information, the secretary of state shall do the following:~~

(1) ~~Criteria for accessing confidential personal information.~~

~~Personal information systems of the secretary of state are managed on a "need-to-know" basis whereby~~ For each personal information system, the information owner shall ~~determines~~determine the level of access required for an employee of the secretary of state to fulfill ~~his/her~~their job duties, consistent with section (C) of this rule. ~~The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior~~ Prior to providing ~~the~~an employee with access to confidential personal information within a personal information system, both the information owner and the employee's supervisor shall grant approval. The ~~secretary of state~~ information owner shall ~~establish~~ revise~~procedures~~

~~for determining a revision to~~ an employee's access to confidential personal information upon a change to that employee's job duties ~~including, but not limited to, transfer or termination~~if appropriate. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the information owner shall remove the employee's access to confidential personal information ~~shall be removed~~.

(2) ~~Individual's request for a list of confidential personal information.~~

Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the agency, the agency shall do all of the following:

(a) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;

(b) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and

(3) ~~Notice of invalid access.~~

(a) Upon discovery or notification that confidential personal information ~~of a person~~ has been accessed by an employee for an invalid reason, the secretary of state shall determine whether it is necessary to delay notification to either person whose information was invalidly accessed for any of the following reasons:~~notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the secretary of state shall delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. Additionally, the secretary of state may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system. "Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information. Once the secretary of state determines that notification would not delay or impede an investigation, the secretary of state shall disclose the access to confidential personal information made for an invalid reason to the person.~~

(i) To ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. "Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information.

(ii) To take any measures necessary to determine the scope of the invalid access, including which individuals' confidential information invalidly was accessed, and to restore the reasonable integrity of the system.

(b) The secretary of state shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time.

~~(b)~~(c) ~~Notification provided by the~~The secretary of state shall inform the person of the type of confidential personal information accessed and the ~~date(s)~~date or dates of the invalid access.

~~(c)~~(d) Notification may be made by using any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

(4) ~~Appointment of a data privacy point of contact.~~

The secretary of state director shall designate an employee of the secretary of state to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the secretary of state with both the implementation of privacy protections for the confidential personal information that the secretary of state maintains and compliance with section 1347.15 of the Revised Code and the rules adopted ~~pursuant to the authority provided by that chapter~~thereunder.

(5) ~~Completion of a privacy impact assessment. The secretary of state shall designate an employee of the secretary of state to serve as the~~The data privacy point of contact ~~who~~ shall complete the privacy impact assessment form developed by the office of information technology.

(C) ~~Valid reasons for accessing confidential person information.~~ Performing any of the following functions ~~constitute~~constitutes a valid ~~reason(s)~~reason for authorized employees of the secretary of state to access confidential personal information:

(1) Responding to a public records request;

(2) Responding to a request from an individual for the list of ~~CPI~~confidential personal information the agency maintains on that individual;

(3) Administering a constitutional provision or duty;

(4) Administering a statutory provision or duty;

(5) Administering an administrative rule provision or duty;

(6) Complying with any state or federal program requirements;

(7) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;

(8) Auditing purposes;

(9) Licensure [or permit, eligibility, filing, etc.] processes;

(10) Investigation or law enforcement purposes;

(11) Administrative hearings;

(12) Litigation, complying with an order of the court, or subpoena;

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

(14) Complying with an executive order or policy;

(15) 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

(16) Complying with a collective bargaining agreement provision.

(D) ~~Confidentiality statutes.~~

The following federal statutes or regulations or state statutes and administrative rules make personal information maintained by the secretary of state confidential ~~and identify the confidential personal information within the scope of rules promulgated by the secretary of state in accordance with section 1347.15 of the Revised Code~~:

(1) ~~Social security numbers:~~ The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (5 U.S.C. 552a). ~~, unless the individual was told that the number would be disclosed.~~

(2) The Driver's Privacy Protection Act, 18 U.S.C. 2721 et seq.

~~(2)~~(3) ~~"Bureau of Criminal Investigation and Information" criminal records check results: section~~Section 4776.04 of the Revised Code.

~~(3)~~(4) ~~Records exempt from disclosure under the~~The Ohio Public Records Act: Chapter 149~~.~~ of the Revised Code.

(5) Section 1306.23 of the Revised Code.

(E) ~~Restricting and logging access to confidential personal information in computerized personal information systems. For personal information systems that are computer systems and contain confidential personal information, the agency shall do the following:~~

(1) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure.

(2) ~~Acquisition of a new computer system.~~ When the secretary of state acquires a new computer system that stores, manages or contains confidential personal information, the secretary of state shall include a mechanism for recording specific access by employees of the secretary of state to confidential personal information in the system.

(3) ~~Upgrading existing computer systems.~~ When the secretary of state modifies an existing computer system that stores, manages or contains confidential personal information, the secretary of state shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the secretary of state to confidential personal information in the system.

(4) ~~Logging requirements regarding confidential personal information in existing computer systems.~~

~~(a) The secretary of state shall require employees of the secretary of state who access confidential personal information within computer systems to maintain a log that records that access.~~

~~(b)~~(a) ~~Access to~~ The secretary of state shall require employees of the secretary of state who access confidential personal information within existing computer systems to ~~is not required to be entered into the~~ maintain a log that records that access exceptunder the following circumstances:

(i) The employee of the secretary of state is accessing confidential personal information for official secretary of state-related purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(ii) The employee of the secretary of state is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iii) The employee of the secretary of state comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iv) The employee of the secretary of state accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(a) The individual requests confidential personal information about ~~himself/herself~~theirself.

(b) The individual makes a request that the secretary of state takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

(c) For purposes of this paragraph, the secretary of state may choose the form or forms of logging, whether in electronic or paper formats.

(F) ~~Log management.~~

(1) The secretary of state shall issue a policy that specifies the following:

(a) Who shall maintain the log;

(b) What information shall be captured in the log;

(c) How the log is to be stored; and

(d) How long information kept in the log is to be retained.

(2) Nothing in this rule limits the agency from requiring logging in any circumstance that it deems necessary.

Effective:

Five Year Review (FYR) Dates: 1/10/2022

_____

Certification

_____

Date

Promulgated Under:	119.03
Statutory Authority:	149.43, 1347.15
Rule Amplifies:	1347.15
Prior Effective Dates:	03/31/2014, 01/25/2016