Ohio Administrative Code

Rule 111-1-02 Confidential personal information systems.

Effective: March 28, 2022

(A) 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 currently in place.

(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.

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

(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)

(1)

For each personal information system, the information owner shall determine the level of access required for an employee of the secretary of state to fulfill their job duties, consistent with paragraph (C) of this rule. Prior to providing 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 information owner shall revise an employee's access to confidential personal information upon a change to that employee's job duties 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.

(2)

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)

(a) Upon discovery or notification that confidential personal information 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:

(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.

(c) The secretary of state shall inform the person of the type of confidential personal information accessed and the date or dates of the invalid access.

(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)

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 thereunder.

(5) The data privacy point of contact shall complete the privacy impact assessment form developed by the office of information technology.

(C) Performing any of the following functions constitutes a valid 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 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)

The following federal statutes or regulations or state statutes and administrative rules make personal information maintained by the secretary of state confidential:

(1) The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

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

(3) Section 4776.04 of the Revised Code.

(4) The Ohio Public Records Act: Chapter 149 of the Revised Code.

(5) Section 1306.23 of the Revised Code.

(E)

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

(2) 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) 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)

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

(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.