# Ohio Administrative Code

## Rule 901-10-02 Procedures for accessing confidential personal information.

Effective: December 12, 2024

For personal information systems, whether manual orcomputer systems that contain confidential personal information, the departmentshall do the following:

(A) Develop criteria for accessing confidential personal information. Personal information systems of the department are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the department to fulfill his/her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The department shall establish 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. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the employee's access to confidential personal information shall be removed.

(B) 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 department, the department shall do all of the following:

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

(2) 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) If all information relates to an investigation about that individual, inform the individual that the department has no confidential personal information about the individual that is responsive to the

individual's request.

(C) Notice of invalid access.

(1) Upon discovery or notification that confidential personal information of an individual has been accessed by an employee for an invalid reason, the department shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the department 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 department 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 department determines that notification would not delay or impede an investigation, the department shall disclose the access to confidential personal information made for an invalid reason to the person.

(2) Notification provided by the department shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access.

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

(D) Appointment of a data privacy point of contact. The director shall designate an employee of the department to serve as the data privacy point of contact (DPPOC). The DPPOC shall work with the chief privacy officer (CPO) within the office of information technology to assist the department with both the implementation of privacy protections for the confidential personal information that the department maintains and compliance with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.

(E) Completion of a privacy impact assessment. The DPPOC in conjunction with the chief privacy

officer and the information owner will timely complete a privacy impact assessment (PIA) form developed by the department of administrative services (DAS) office of information technology. The form is posted at https://das.ohio.gov/technology-and-strategy/information-security-privacy/privacy.

(F) Training:

(1) The policy regarding the rules adopted under Chapter 901-10 of the Administrative Code will be distributed to all employees and they will be required to acknowledge receipt.

(2) The policy will be posted on the department's intranet.

(3) A poster summarizing the department's policy will be posted in a conspicuous place in the main office of the department and in all locatons where the department has branch offices.