Ohio Administrative Code

Rule 3334-1-16 Procedures for accessing confidential personal information.

Effective: March 7, 2011

For personal information systems, whether manual or computer systems that contain confidential personal information, the authority shall do the following:

(A) Criteria for accessing confidential personal information. Personal information systems of the authority are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the authority to fulfill his/her job duties. The determination of access to confidential personal information shall be approved by the employees supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The authority shall establish procedures for determining a revision to an employees access to confidential personal information upon a change to that employees job duties including, but not limited to, transfer or termination. Whenever an employees job duties no longer require access to confidential personal information in a personal information system, the employees access to confidential personal information shall be removed.

(B) Individuals 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 authority, the authority 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 Ohio tuition trust authority has no confidential personal information about the individual that is responsive to the individuals request.

(C) Notice of invalid access.

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

(2) Notification provided by the authority 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 authoritys executive director shall designate an employee of the authority 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 authority with both the implementation of privacy protections for the confidential personal information that the authority 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 authoritys executive director shall designate an employee of the authority to serve as the data privacy point of contact who shall timely complete the

privacy impact assessment form developed by the office of information technology.