3737-1-23 **Access and maintenance of confidential personal information.**

For purposes of confidential personal information that is maintained by the board, the following definitions apply:

(A) Definitions:

(1) "Access" as a noun means an instance of copying, viewing, or otherwise perceiving whereas "access" as a verb 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 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 this rule addressing requirements in section 1347.15 of the Revised Code.

(3) "Computer system" means hardware, software, and other equipment that stores, maintains, or retrieves personal information using electronic data processing.

(4) "Confidential personal information" has the same meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by paragraph (D) of this rule.

(5) "Employee of the board" means each employee of the board regardless of whether he/she holds an appointed office or position within the board. "Employee of the board" is limited to the petroleum underground storage tank release compensation board.

(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 contact" 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 of the board and maintained by the board for internal administrative and human resource purposes.

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

(16) "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) For personal information systems, whether manual or computer systems that contain confidential personal information, the following rules apply:

(1) Criteria for accessing confidential personal information. Employees of the board are authorized to access personal information systems for valid reasons in accordance with paragraph (C)(1) of this rule to the extent required to perform assigned job duties;

(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 board, the employee responding to such request 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

(c) If all information relates to an investigation about that individual, inform the individual that the board has no confidential personal information about the individual that is responsive to the individual's request.

(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 board shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, notification shall be delayed 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 board may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individual's confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system.

(b) "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 board determines that notification would not delay or impede an investigation, the board shall disclose the access to confidential personal information made for an invalid reason to the person.

(c) Notification shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access.

(d) Notification may be made by any method reasonable 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 director shall designate an employee 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 with both the implementation of privacy protections for the confidential personal information that the board maintains as well as work to ensure compliance with section 1347.15 of the Revised

Code and this rule.

(5) Completion of a privacy impact assessment. The director shall designate an employee 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.

(C) Pursuant to the requirements of division (B)(2) of section 1347.15 of the Revised Code, this rule contains a list of valid reasons, directly related to the board's exercise of its powers or duties, for which only employees of the board may access confidential personal information regardless of whether the personal information system is a manual system or computer system:

(1) Performing the following functions constitutes valid reasons for authorized employees of the board to access confidential personal information:

(a) Responding to a public records request;

(b) Responding to a request from an individual for the list of confidential personal information the board maintains regarding that individual;

(c) Administering a constitutional provision or duty;

(d) Administering a statutory provision or duty;

(e) Administering an administrative rule, provision or duty;

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

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

(h) Auditing purposes;

(i) Investigation or law enforcement purposes;

(j) Administrative hearings;

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

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

(m) Complying with an executive order or policy; or

(n) Complying with an agency policy or state administrative policy issued by the department of administrative services, the office of budget and management or other similar agency.

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

(1) Social security numbers: 5 U.S.C. 552a . , "State ex rel Beacon Journal v. Akron (1994), 70 Ohio St. 3d 605.", unless the individual was told that the number would be disclosed.

(2) Records exempt from disclosure under the Ohio Public Records Act: Chapter 149. of the Revised Code.

(E) For personal information systems that are computer systems and contain confidential personal information, the board 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 board acquires a new computer system that stores, manages or contains confidential personal information, the board shall include a mechanism for recording specific access by employees of the board to the system.

(3) Upgrading existing computer systems. When the board modifies an existing computer system that stores, manages or contains confidential personal information, the board 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 board to confidential personal information in the system.

(4) Logging requirements regarding confidential personal information in existing

manual and computer systems.

(a) The board shall require employees of the board who access confidential personal information within the computer system to maintain a log that records that access.

(b) Access to confidential information is not required to be entered into the log under the following circumstances:

(i) The employee of the board is accessing confidential personal information for official authority 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 board 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 board 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 board accesses confidential personal information to the extent necessary to perform assigned job duties and the access is for a valid reason as defined in paragraph (C)(1) of this rule.

(v) The employee of the board 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.

(b) The individual makes a request that the board 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 director may choose the form or forms of logging, whether in electronic or paper formats.

(F) Log management. The director or designee shall maintain an electronic or paper log that records access to confidential personal information on existing computer systems for any reason not specified in paragraph ~~(D)(4)(b)~~ (E)(4)(b) of this rule. The director shall issue a policy that specifies the following:

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

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

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