991-9-01 **Accessing Confidential Personal Information.**

Chapter 991-09 regulates employee access to the confidential personal information that OEC retains. OEC has promulgated this chapter in response to section 1347.15 of the Revised Code.

(A) Definitions for Chapter 991-09 of the Administrative Code:

(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.

(3) "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, 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 rule 991-09-01 of the Administrative Code.

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

(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) "OEC" means "the Ohio Expositions Commission."

(10) "Person" means a natural person.

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

(12) "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.

(13) “Research” means a methodical investigation into a subject.

(14) “Routine” means commonplace, regular, habitual, or ordinary.

(15) “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 OEC for internal administrative and human resource purposes.

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

(17) “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 confidential personal information.

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

(1) Criteria for accessing confidential personal information: Personal information systems of OEC are managed on a “need-to-know” basis whereby the information owner determines the level of access required for an employee of OEC to fulfill his or 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. OEC 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.

(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 OEC, OEC 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 OEC 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, OEC shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, OEC 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, OEC 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 OEC determines that notification would not delay or impede an investigation, OEC shall disclose the access to confidential personal information made for an invalid reason to the person.

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

(c) Notification may be made by 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: OEC's executive director shall designate an OEC 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 OEC with both the implementation of privacy protections for the confidential personal information that OEC maintains and compliance with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that

chapter.

(5) Completion of a privacy impact assessment: OEC's executive director shall designate an OEC 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) Valid reasons for accessing confidential personal information.

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 OEC's exercise of its powers or duties, for which only employees of the agency may access confidential personal information (CPI) regardless of whether the personal information system is a manual system or computer system. Performing the following functions constitute valid reasons for authorized employees of the agency 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 that OEC 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 (or monitoring, reviewing, etc.) purposes;

(9) Investigation or law enforcement purposes;

(10) Administrative hearings;

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

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

(13) Complying with an executive order or policy;

(14) 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

(15) Complying with a collective-bargaining agreement provision.

(D) Confidentiality statutes and regulations.

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

(1) 5 U.S.C. 552a for social security numbers;

(2) 45 C.F.R. 160, 45 C.F.R. 162, and 44 C.F.R. 164 for the privacy of individually-identifiable health information (HIPPA);

(3) Section 149.43 of the Revised Code for the general statute on public records;

(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, OEC 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 OEC acquires a new computer system that stores, manages, or contains confidential personal information, OEC shall include a mechanism for recording specific access by employees of the agency to confidential personal information in the system.

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

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

(a) OEC shall require employees of the agency who access confidential personal information within computer systems 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 OEC is accessing confidential personal information for official agency 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 OEC 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 OEC 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 OEC 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 or herself.

(b) The individual makes a request that OEC take 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 paragraph (4) of this rule, OEC may choose the form or forms of logging, whether in electronic of paper formats.

(5) Log management: Nothing in this rule limits OEC from requiring logging in any circumstance that it deems necessary. OEC 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.

Effective:

R.C. 119.032 review dates:

_____

Certification

_____

Date

Promulgated Under:	119.03
Statutory Authority:	1347.15
Rule Amplifies:	1347.15