Ohio Arts Council

30 EAST BROAD STREET, 33rd FLOOR
COLUMBUS, OHIO 43215-3414
614-466-2613
OAC.OHIO.GOV

Standard Operating Procedure
Incident Response for Access of Confidential or Sensitive Personally Identifiable Information for an Invalid Reason

---

1. Purpose:
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the Ohio Arts Council (OAC) when Confidential Personal Information (CPI) or Sensitive Personally Identifiable Information (SPII) that is contained in an OAC-managed system is accessed for an invalid reason by an OAC employee or contractor. This document sets forth the procedures for processing illegal activity and wrongdoing, and provides for the careful, expeditious handling of all allegations and claims of improper access. The procedure covers both electronic and paper-based CPI and SPII.

2. Overview:
   Ohio Revised Code Section (ORC) 1347.15 (B)(6) requires a state agency to have a procedure to notify each person whose CPI has been accessed for an invalid reason by employees of the state agency. Depending on the circumstances, state and federal laws require notification of affected individuals when there has been a security breach or invalid access for particular types of PII. However, it is not always clear whether a given incident is in fact a breach or other notification-triggering event. This procedure requires employees and contractors to report incidents so that the agency may make a determination of the steps that need to be taken.

   For purposes of this procedure:

   - "Personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:
     - a name, identifying number, symbol, or other identifier assigned to a person,
     - any information that describes anything about a person,
     - any information that indicates actions done by or to a person,
     - any information that indicates that a person possesses certain personal characteristics.

     It includes "personal information" as defined by ORC 1347.01. Some examples of personally identifiable information are:
     - names
     - Social Security numbers
     - resumes
     - contracts
     - correspondence
     - addresses
     - phone numbers
     - driver's license numbers
     - state identification numbers
     - professional license numbers
     - financial account information
     - medical and health information
     - physical characteristics and other biometric information
     - education information
     - tax information
     - individuals' job classifications and salary information
     - performance evaluations
     - employment application forms
     - timesheets

- "Sensitive personally identifiable information" includes personally identifiable information that OAC has discretion not to release under public records law, and it also includes "confidential personal information," which OAC is restricted or prohibited from releasing under Ohio's public records law. Examples of "sensitive personally identifiable information" that OAC keeps includes:
    - Social Security numbers
    - a person's financial account numbers and information
    - beneficiary information
    - tax information
    - employee voluntary withholdings
    - passwords
    - employee home addresses and phone numbers
    - employees' non-state-issued email addresses
    - medical and health information
    - state ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
    - confidential personal information (see below)

- "Confidential personal information" is personal information that falls within the scope of section 1347.15 of the Revised Code and that the OAC is prohibited from releasing under Ohio's public records law. It applies to Social Security numbers, fingerprint data and medical and health information that is maintained in the following personal information systems only:
    - OAKS
    - Hard-copy personnel records
    - Hard-copy individual artist records

NOTE: the OAC also maintains an electronic grant management system, however, this system does not contain any confidential personal information on OAC grant applicants.

- "Illegal Activity" as used in this procedure includes fraud, theft, assault and other violations of local, state or federal law, including violations of state ethics laws, committed or in the process of being committed, by a state employee on any property owned or leased by the state or during the course of executing official duties.
- The term "incident" refers to facts and circumstances that lead to a reasonable belief that there has been an access of CPI or SPII for an invalid reason that affects one or more computer systems, networks, or other components of the OAC technology infrastructure, or to the threat of such an event.
- "Invalid reason" means any basis for access that is not directly related to the OAC's exercise of its powers or duties as described in the agency's CPI access policies. Ohio Administrative Code 3379-15-03 identifies valid reasons for accessing CPI within the OAC.
- "Wrongdoing" as used in this procedure includes a serious act or omission, committed by a state employee on any property owned or leased by the state or during the course of executing official duties. Wrongdoing is conduct that is not in accordance with standards of proper governmental conduct and which tends to subvert the process of government, including, but not limited, to gross violations of departmental or agency policies and procedures, executive orders, and acts of mismanagement, serious abuses of time, and other serious misconduct. For purposes of this reporting procedure, wrongdoing does not include illegal or suspected illegal activity. Likewise, wrongdoing does not include activity that is most appropriately handled through the department's human resources personnel.

3. Response to access of CPI or SPII for an invalid reason:

   A. Responsibilities: OAC employees and contractors have the following responsibilities when making a report of access of CPI or SPII for an invalid reason:

      a. Employees and contractors shall report incidents of suspected access of CPI or SPII for an invalid reason to a manager. If an employee or contractor is unable to report the suspected incident to a manager, the report should be made to the Data Privacy Point of Contact (DPPOC), the OAC's Assistant Attorney General, or the Administrator for the program area involved.

      b. Managers or the party that received the initial report shall notify the DPPOC, the deputy director, of the suspected incident.

      c. The DPPOC shall notify the executive director that a suspected incident has occurred and will be reviewed. The DPPOC will then coordinate a review of the suspected incident to determine if:

         i. A security breach as defined by ORC 1347.12 has occurred, where "breach" is defined as unauthorized access to computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.
         ii. A violation of ORC 1347.15 has occurred, where CPI has been accessed for an invalid reason by an agency employee.
         iii. A violation of another regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), has occurred, or that there is some other risk or threat that makes notification of affected parties appropriate.

         The DPPOC will involve the following parties in this review:

         - Agency human resources representative;
         - Agency administrator of the program area involved;
         - Agency chief information officer or lead administrator;
         - OAC Assistant Attorney General; and
         - Other parties as deemed appropriate.

      d. If the review of the suspected incident determines that CPI or SPII has been inappropriately accessed, the OAC Assistant Attorney General shall report the incident in the following manner:

         - Notify the OAC executive director and/or deputy director.
         - Notify the Governor's Office.
         - Notify the Ohio Customer Service and Security Center (OCSSC) at 614-644-0701 or toll free at 800-644-0701.
         - Notify the Ohio State Highway Patrol.

         If there is clear danger and the agency Chief Legal Counsel is not available, the DPPOC can also contact the Ohio State Highway Patrol at 1-877-772-8765.

e. The deputy director is responsible for notifying all individuals affected by CPI or SPII upon a finding that notification is required or prudent.

f. Employees and contractors should avoid reporting a suspected incident of access to CPI or SPII for an invalid reason to those parties suspected of performing or ordering such access.

g. Although employees are reminded of their duty to comply with the whistleblower statutes ORC 124.341 and ORC 4113.52, employees who report an access of CPI or SPII that they believe is for an invalid reason should have a reasonable factual basis for believing that improper activities have occurred. They should provide as much specific information as possible to allow for proper assessment of the nature, extent, and urgency of the incident.

4. Requests for Incident Information:
   If an OAC employee or contractor receives a request for incident information directly from the public, or from any other individual who is not associated with the incident resolution, the OAC employee or contractor will provide no information and will direct the request to the OAC Public Information Office, who will coordinate any public statements.

5. Training:
   A review of this procedure will be included on the agenda of an annual staff meeting. In addition, new employees must receive training on this standard operating procedure prior to accessing any OAC system that contains CPI.

6. Maintenance of this Procedure:
   This procedure will be reviewed at least once annually to ensure it remains compliant with ORC 1347.15 and with any corresponding OAC policy.

7. Revision History:

Date	Description
05/22/2012	New standard operating procedure
7/1/2013	Review