



Standard Operating Procedure Accessing and Logging Confidential Personal Information in a Computer-Based System

Ohio Arts Council
OAKS system

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 accessing Confidential Personal Information contained in OAKS system, which is managed by the OAC Fiscal Office in consultation with the Ohio Office of Budget And Management (OBM).

2. Overview

All state agencies, boards and commissions are required to implement Ohio Revised Code Section 1347.15 that includes provisions to protect the privacy and security of Ohio's citizens who have confidential personal information stored in a state-maintained personal information system. The OAC has issued administrative rules (OAC 3379-15) regulating access to confidential personal information. This procedure applies those rules to the OAKS system.

For purposes of this procedure:

- "Personal information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
- "Confidential personal information" (CPI) is the data identified in section 3. H of this procedure.

3. System Description

A. Name: OAKS

B. Description: A web-based financial and personnel system.

C. Purpose: To pay employees and vendors and maintain fiscal information.

D. Regulatory requirements: Chapter 126 of the Ohio Revised Code.

E. Authorizing access: Employees who need access to the OAKS system are given passwords by the OAKS system, upon approval of the executive director of the Ohio Arts Council.

F. Security: Each OAC employee who needs access to the OAKS system is assigned a password that allows them to complete their assigned tasks.

G. Positions that access the system:

Position title	Permission level (Full access, limited access, etc.)	Sensitive data accessible with this permission level
Fiscal Spec	Full	All
Info Technologist	Limited	Limited (for financial reports, etc.)
Grants Associate	Limited	Limited (determine payment status, etc.)
Executive Director	Limited	Limited (vendor payments, etc.)

H. Description of Sensitive Data Contained in this System: All employee information (Social Security numbers and medical and health information) as well as all financial information about vendors.

I. Valid Reasons for Accessing Sensitive Data: Payment of bills, verification of payment, and processing of payroll.

4. Logging Access to Confidential Personal Information:

A. Logging requirements:

If manual logging is employed, use the attached form to log the following: 1) name (or identifier) of the person whose CPI was accessed, and 2) the date. The logging requirement applies whenever access is targeted to a specifically named individual or group of specifically named individuals and does not otherwise come within an exception. In addition, logging is required under the following conditions:

- i. Access in a system containing CPI to accomplish job duties.
- ii. Access in a system containing CPI because of another state employee's request for information.
- iii. Public record requests that require accessing a system containing CPI.

B. Manual logging exceptions:

Manual logging is not required under the following conditions:

- i. Self service access or request to view own CPI. No logging is necessary when a person views his or her own records containing CPI. For example, an agency applicant who makes a request to review his or her file would not trigger a logging requirement for a staff member fulfilling the constituent's request.
- ii. General Research. When conducting general research, employees do not need to log access if the research is not directed toward a specific-named individual or a group of specifically named individuals. For example, running a report that lists applicants received from 1996 to 2009 and does not target a specifically named applicant is excluded from the logging requirement. The Public Information Office does, however, maintain a log of requests that do name a specific applicant(s).

- iii. Routine office procedures. Logging is not required when performing routine office tasks that are not directed toward specific individuals or groups of specifically named individuals. For example, running a report that uses parameters other than names, such as dates, without the intention of retrieving the information of a specific employee is excluded from the logging requirement. However, using specific search parameters without a name but with the intent to retrieve a specifically named individual still triggers the logging requirement.
- iv. Incidental contact. Logging is not required when an employee incidentally accesses CPI and the contact is merely a result of exposure to the information rather than the primary reason for the access. For example, if a desktop support employee is asked to correct a problem in a system and happens to see CPI because it is already on the screen, the desktop support employee is not required to log access to the CPI because the support employee is not targeting an individual's CPI.
- v. Information requested by an individual about that individual. Logging is not required when an individual requests information about that individual. For example, if John Smith requests information on himself, no logging is required. The individual's request for action also serves as the individual's approval to access the information. In addition, "individual" means a natural person, an authorized representative, legal counsel, legal custodian or legal guardian of the individual. Steps should be taken to ensure that the individual is authorized to make the request and has provided credentials for self or to affirm the relationship.
- vi. Automated logging. Manual logging is not required when the user's access to CPI is recorded by an automated mechanism. Any upgrade of a system or acquisition of a new system must include an automated recording mechanism. This mechanism shall include:
 - Application** – Name of the application generating the log
 - Date** – The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY)
 - Time** – The time the event occurred (HH:MM:SS)
 - Time Zone** – GMT time and offset (if Time not in EST/EDT)
 - Username** – The name of the user accessing the application or attempting to access the application
 - Person** – The name/identifier of the person whose CPI was accessed

C. Use and maintenance of a "Log of Access of Confidential Personal Information": If manual logging is necessary, employees shall use the attached log to list each incident when CPI has been accessed for a specifically named individual or group of specifically named individuals.

D. Retention and destruction of a CPI log: OAKS logs' retention and destruction schedules are managed by OBM.

5. Reporting Suspicious or Inappropriate Requests

Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See *Incident Response for Access of Confidential or Sensitive Personally Identifiable Information for an Invalid Reason*.

6. Training

A review of this procedure will be included on the agenda of an Ohio Arts Council staff meeting at least once annually. In addition, new employees must receive training on this standard operating procedure prior to accessing the OAKS system which contains CPI, followed by a signed statement detailing training received.

7. Maintenance of this Procedure

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15 and with any corresponding OAC policy.

8. Revision History

Date	Description
05/22/2012	New standard operating procedure

Ohio Arts Council
Log of Access of Confidential Personal Information

Name of Personal Information System:	
Name of Person Accessing Confidential Personal Information (CPI):	

Acknowledgment: I acknowledge that the information on this log is true and complete and that (check one):

I have accessed CPI only for purposes relating to my job duties or my agency's governmental function.

I have not knowingly accessed CPI or directed access to CPI that would be logged under the agency Policy on Logging Access to Confidential Personal Information during the following monthly periods: (month/day/year) ___/___/___ to ___/___/___.

Initials: _____ Date of Acknowledgement: _____

Check here if this access log contains confidential information:

	Name (or identifier) of person whose CPI was accessed	Date
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		