



**Standard Operating Procedure
Accessing Sensitive Data**

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 sensitive data contained in the OAKS system which is managed by the OAC Fiscal Office.

2. Overview

This procedure only addresses the access of sensitive data, which may include sensitive personally identifiable information (SPII). For purposes of this procedure:

- “Sensitive data” is the data identified in section 3 H of this procedure.
- “Sensitive personally identifiable information” includes personally identifiable information that OAC has discretion not to release under public records law. For purposes of this procedure, it does not include “confidential personal information” under Ohio Revised Code 1347.15. Examples of “sensitive personally identifiable information” that the OAC keeps may include:

- Social Security numbers or Tax id numbers
- passwords
- employee home addresses and phone numbers
- tax information
- medical and health information

3. System Description

A. Name: OAKS system.

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

C. Purpose: To pay employees and vendors and maintain fiscal information in accordance with state and federal mandates and standards.

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 OAC executive director.

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
Executive Director	Limited	Limited
Info Technologist	Limited	Limited
Grants Tech	Limited	Limited

H. Description of Sensitive Data Contained in this System: All employee 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. Reporting Suspicious or Inappropriate Requests

Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that sensitive data may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See *IT Policy (4), "Security Incident Response."*

5. Training

A review of this procedure will be included on the agenda of annual OAC staff meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing the OAKS system which contains sensitive data.

6. Maintenance of this Procedure

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

7. Revision History

Date	Description
05/22/2012	New standard operating procedure