Office of Information Technology | Office of Information Security and Privacy
Service · Support · Solutions

Ohio Privacy Policies Framework

Instructions for Using Privacy Policy and Procedure Templates

The purpose of the Ohio Privacy Policy and Procedure templates is to help state agencies develop a secure and consistent approach to accessing and handling personally identifiable information. Ohio Revised Code 1347.15 requires state agencies to establish administrative rules regulating access to Confidential Personal Information (CPI). Such rules are implemented in agencies through policies and procedures that provide specific guidance on appropriate privacy practices. Furthermore, agencies are likely to have personally identifiable information that is not covered by ORC 1347.15. For these reasons, the accompanying templates serve as a privacy policy and procedure framework for agencies looking to develop or revise their agency's privacy policies and procedures. Use of the templates also helps ensure both ORC 1347.15 compliance and consistent privacy protections to all types of personally identifiable information.

The framework consists of:

- An overarching policy on protecting privacy and all forms of personally identifiable information.
- A procedure for each system containing either CPI or sensitive data.
- Two agency-wide procedures that address: a) notification of improper CPI access and b) handling requests for personally identifiable information.

When your agency's policy development process is complete, you will have established a policy framework similar to that shown in Figure 1:

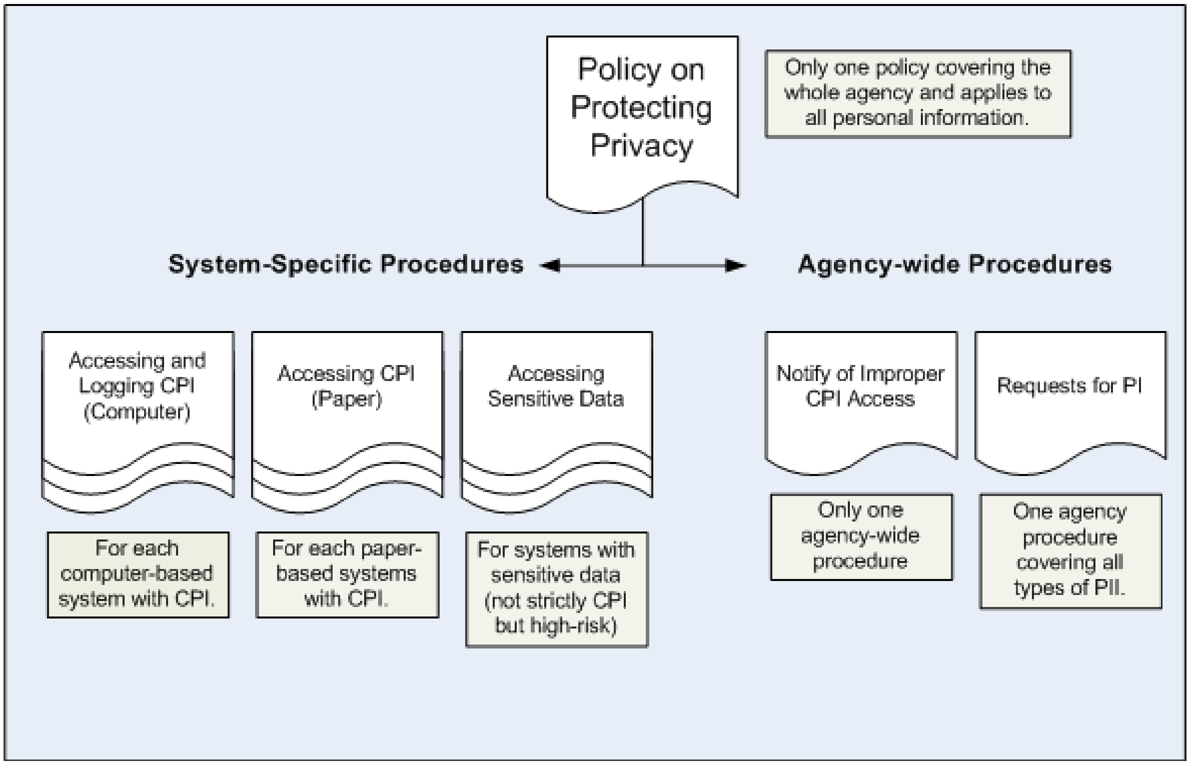
Policy on Protecting Privacy
Only one policy covering the whole agency and applies to all personal information.
System-Specific Procedures
Agency-wide Procedures
Accessing and Logging CPI (Computer)
Accessing CPI (Paper)
Accessing Sensitive Data
Notify of Improper CPI Access
Requests for PI
For each computer-based system with CPI.
For each paper-based systems with CPI.
For systems with sensitive data (not strictly CPI but high-risk)
Only one agency-wide procedure
One agency procedure covering all types of PII.

Figure 1: Privacy Policy and Procedure Framework

Published: November 18, 2011

State agencies are free to use or not use these templates, in whole or in part, although they must still meet the requirements of ORC 1347.15. The templates require a level of customization that reflects the individual agency's data collection practices, appropriate uses, and systems.

To customize the privacy policy and procedure templates to your agency's particular business processes, please use the following instructions as a developmental guide. Note that certain procedures or sections may be unnecessary based on the types of personally identifiable information maintained by your agency.

1. Use any existing documentation. For example, work with the agency's business leaders to obtain an inventory of your agency's information systems, both electronic and paper, that contain sensitive data or CPI. Or, examine the Privacy Impact Assessments for your agency's systems.

2. Using the information in the PIAs, complete a standard operating procedure for each system identified in the inventory. Create one standard operating procedure for each system as follows:

   a. For each electronic system that contains CPI, create a standard operating procedure based on the template, "*Accessing and Logging Confidential Personal Information in a Computer-Based System*." (Use "Template – Accessing and Logging CPI.doc").

   b. For each paper-based system that contains CPI, create a standard operating procedure based on the template "*Accessing Confidential Personal Information in a Paper-Based System*." (Use "Template – Accessing CPI Paper Template.doc").

   c. For each system containing sensitive data that is not within the scope of ORC 1347.15, create a standard operating procedure based on the template "*Accessing Sensitive Data*." (Use "Template – Accessing Sensitive Data.doc"). This procedure is for systems that do not contain CPI but do hold high-risk information that warrants additional precautions.

Once you have completed standard operating procedures for each system that contains sensitive data or CPI within your agency, begin development of the agency-wide ORC 1347.15-related policy and procedures. The Office of Information Security and Privacy recommends that state agencies develop each of the following documents, even if no CPI is maintained by the agency:

3. Create a single, agency-wide standard operating procedure based on the template "*Request to Inspect Personally identifiable Information*." Note that you will need to provide a list of the agency's CPI systems within this standard operating procedure. (Use "Template – Requests for PI.doc").

4. Create a single, agency-wide standard operating procedure based on the template "*Incident Response for Access of Confidential or Sensitive Personal Information for an Invalid Reason.*" Note that you will need to provide a list of the agency's CPI systems within this standard operating procedure as well as reference your agency's procedure for security incident response. (Use "Template – SPI-CPI Incident Response.doc").

5. Create a single, agency-wide policy based on the template "*Policy on Protecting Privacy*." This policy will apply to all types of personally identifiable information that the agency maintains. You will need to provide a list of the agency's CPI systems, identify the types of CPI contained in these systems, and reference other agency policies or procedures within this document. (Use "Template – Policy on Protecting Privacy.doc").

These templates and additional resources are available at http://privacy.ohio.gov/Government under "ORC 1347.15 Guidance."

This guidance was developed by the Chief Privacy Officer for the State of Ohio in consultation with the Ohio Privacy Advisory Board. Please contact Office of Information Security and Privacy at (614) 644-9391 or at chief.privacy.officer@oit.ohio.gov if you have any questions about these templates.

Template for “Policy on Protecting Privacy”

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the policy for your agency.
3) Check to ensure that this box and “add information here” type language have been replaced.
4) Place the procedure text into your agency’s procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services’ Office of Information Technology.

POLICY ON PROTECTING PRIVACY

POLICY NUMBER:	EFFECTIVE DATE:	APPOINTING AUTHORITY APPROVAL:

1. PURPOSE

The *(add agency name here)* takes seriously the protection of personally identifiable information. This policy provides the requirements for protecting the privacy of people who have personally identifiable information in our databases, electronic and paper files and other records. This policy covers all *(add agency name here)* employees. It also covers contractors who gain access to *(add agency name here)* physical facilities or data or computer systems. This policy lays out basic handling expectations first for all types of personally identifiable information, and second, it provides important additional handling requirements for sensitive personally identifiable information.

What is “Personally Identifiable Information” and What is “Sensitive Personally Identifiable Information”?

For the purposes of this policy, “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 Ohio Revised Code (ORC) 1347.01. Some examples of personally identifiable information are *(add and remove types of personally identifiable information to tailor the list to your agency)*:

- names
- Social Security numbers
- resumes
- 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
- tax information
- education information
- individuals’ job classifications and salary information
- performance evaluations
- employment application forms
- timesheets

“Sensitive personally identifiable information” includes personally identifiable information that *(add agency name here)* has discretion not to release under public records law, and it also includes “confidential personal information,” which *(add agency name here)* is restricted or prohibited from releasing under Ohio’s public records law. Examples of “sensitive personally identifiable information” that *(add agency name here)* keeps includes *(add and remove types of sensitive personally identifiable information to tailor list to your agency)*:

- 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
- security challenge questions and answers
- employees’ non-state-issued email addresses
- medical and health information
- fingerprints and other biometric information
- driver’s license numbers
- 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 *(add agency name here)* is prohibited from releasing under Ohio’s public records law. It applies to *(list your agencies confidential personal information here if possible or cross-reference list)* that is maintained in the following *(add number of systems here)* personal information systems only:

- (add system name) – (add division name) (indicate whether system is computer-based or paper-based)

2. POLICY

(Add agency name here) employees and contractors as outlined above must follow these rules on handling all personally identifiable information and handling sensitive personally identifiable information whenever they know or have reason to know that the

information is personally identifiable information or sensitive personally identifiable information.

A. Handling All Personally Identifiable Information

i. Use personally identifiable information only for official, lawful purposes.
ii. Do not access systems with personally identifiable information – whether electronic or paper – if you have not been authorized to do so. Contact your supervisor if you need access.
iii. Enter personally identifiable information accurately. Make a good faith effort to correctly enter data. Never intentionally enter false data.
iv. Take reasonable precautions to protect personally identifiable information from unauthorized modification, destruction, use or disclosure. Follow *(add agency name here)* information security policies and procedures.
v. Whenever an individual requests information that *(add agency name here)* maintains about that individual, employees and contractors shall follow *(add agency name here)* Standard Operating Procedure – Request to Inspect Personally Identifiable Information.
vi. Only collect personally identifiable information when you have been authorized to do so by the proper *(add agency name here)* manager. Do not create an electronic or paper system of record with personally identifiable information unless you have *(add agency name here)* authorization and follow *(add agency name here)*-mandated privacy and security requirements *(or reference named procedure)*.
vii. Destroy personally identifiable information securely in accordance with records retention schedules and following *(add agency name here)* data destruction procedures for particular systems or records *(or reference named procedure)*.
viii. Do not initiate or otherwise contribute to any disciplinary or other punitive action against any individual who reports evidence of unauthorized use of personally identifiable information.
ix. *(Add agency name here)* monitors its information, systems, other IT assets, employees and contractors for compliance with this policy. Therefore, employees and contractors have no expectation of privacy when they use state information, systems and IT assets.

B. Handling Sensitive Personally identifiable information

i. **Only access sensitive personally identifiable information for a valid reason directly related to the exercise of a *(add agency name here)* power or duty.** Valid reasons include *(add reasons specific to your agency's lines of business)*:
    - Responding to a public records request;
    - Responding to a request from an individual for the list of personally identifiable information the agency maintains on that individual;
    - Administering a constitutional provision or duty;
    - Administering a statutory provision or duty;
    - Administering an administrative rule provision or duty;
    - Complying with any state or federal program requirements;
    - Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
    - Auditing purposes;

- Carrying out licensure, permit, eligibility, filing, certifications or other similar processes;
- Carrying out or assisting with an authorized investigation or law enforcement purposes;
- Conducting or preparing for administrative hearings;
- Responding to or preparing for litigation, or complying with a court order or subpoena;
- Administering human resources, including but not limited to hiring, promotion, demotion, discharge, salary and compensation issues, leave requests and related issues, time card approvals and related issues;
- Administering an information system;
- Complying with an executive order or policy;
- 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
- Complying with a collective bargaining agreement provision.

ii. **Do not access or use sensitive personally identifiable information for any reason other than those listed above.** For example, do NOT access or use sensitive personally identifiable information:

- for gain or personal profit for yourself or someone else,
- out of simple curiosity or personal interest,
- to commit a crime,
- for retribution, use in a personal conflict, or promotion of a personal point of view, or
- to harass or embarrass.

iii. **You always have a duty not to disclose sensitive personally identifiable information without proper agency authorization.** As you do your work, you may inadvertently or unintentionally come in contact with information that you know or have reason to believe is sensitive personally identifiable information. In those circumstances, you have a duty not to disclose that sensitive personally identifiable information to anyone except properly authorized persons.

iv. **If you suspect that sensitive personally identifiable information has been improperly accessed or disclosed, you shall report the incident to your manager or another manager or contact the *(add agency name here)* Data Privacy Point of Contact at *(add phone number here)*.**

- Report quickly and do not disturb evidence.
- Allow the *(add agency name here)* response team to preserve evidence, eliminate any ongoing risks and make a determination that violations have occurred.
- To ensure that any investigation is not compromised and that an accurate evaluation of the incident is conducted, only the director, assistant directors or deputy directors of *(add agency name here)* may authorize notifications to affected individuals.
- Upon a finding that confidential personal information has been access for an invalid reason in violation of a confidentiality statute, section 1347.15 of the Revised Code or rules *(add administrative rule references here)* of the

Administrative Code, the director, assistant directors or deputy directors of *(add agency name here)* will notify affected individuals.

v. Because confidential personal information (CPI) requires a higher standard of care, employees accessing the following **CPI systems** shall follow the privacy procedure specific to that system:
   - o See *(add agency name here) (add procedure name here)*.

vi. Nothing in this policy restricts the release of public records. Personally identifiable information is only sensitive if Ohio law gives the agency discretion on its release. Personal information is only confidential if Ohio law prohibits the agency from its release.

3. Violations

i. Any employee who violates this policy is subject to disciplinary action up to and including termination.
ii. Any employee who violates a confidentiality statute or *(add agency name here)* rules *(add administrative rule references here)* is subject to criminal charges, civil liability arising out of the employee's actions, employment termination and a lifelong prohibition against working for the State of Ohio.
iii. Any violation of this policy by a contractor may be considered a material breach of the contract and may subject the contract to termination. Any contractor who violates a confidentiality statute may also be subject to criminal charges and civil liability arising out of the contractor's actions. The vendor may also be subject to vendor debarment.
iv. An employee or contractor who complies in good faith with this policy is not subject to discipline under this policy.
v. This policy does not prohibit an employee from accessing information about himself or herself as long as the person has been granted access to the system and uses authorized processes, or makes a request to *(add agency name here)* for a list of the personally identifiable information that the department maintains about himself or herself.

4. Maintenance of This Policy

This policy will be reviewed at least once annually to ensure that it remains compliant with Federal and State privacy laws including ORC Section 1347.15 and that it accurately reflects *(add agency name here)* personally identifiable information and systems.

5. Questions

For questions regarding this policy, please contact the *(add agency name here)* Data Privacy Point of Contact at *(add phone number here)*.

6. Revision History

Date	Description
MM/DD/YYYY	New policy

[Place on agency letterhead or procedure template]

Template for "Accessing and Logging Confidential Personal Information in a Computer-Based System"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

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

Insert office name here
Insert name of system here

1. Purpose
This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add name of office here)* when accessing Confidential Personal Information contained in *(add name of system here)* which is managed by the *(add name of office here)*.

2. Overview
All state agencies, boards and commissions are required to implement Ohio Revised Code Section 1347.15 which 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 *(department name)* has issued administrative rules *(add citation to rules)* regulating access to confidential personal information. This procedure applies those rules to *(add system name here)*.

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
   Note: Complete items A-I below. Add additional items as warranted to provide a full description of this system and the CPI that must be managed.

   A. Name: *provide the name of the system here.*

   B. Description: *provide a description of the system of record here, including an overview of the application used or the platform on which it resides.*

   C. Purpose: *explain why this system is maintained and the purpose it serves.*

   D. Regulatory requirements: *list the citation(s) (state or federal laws or rules) that require or support the existence and maintenance of this system.*

   E. Authorizing access: *explain who authorizes access to the system, how those authorizations are maintained and how those authorizations are revoked when an employee terminates service or otherwise no longer needs access to CPI in the system.*

   F. Security: *explain the security controls that exist with this system such as passwords or other forms of authentication.*

   G. Positions that access the system:

Position title	Permission level (Full access, limited access, etc.)	CPI accessible with this permission level

   H. Description of CPI Contained in this System: *Provide a list of the CPI contained in this system along with the federal or state statutes or administrative rules that make the confidential personal information confidential.*

   I. Valid Reasons for Accessing CPI: *List the valid business reasons as to why this system is used. Be sure to also include the valid reasons for accessing CPI.*

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:

   (Specify the appropriate actions for logging CPI given each of the following scenarios:)

   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 customer who makes a request to review his or her case file would not trigger a logging requirement for a caseworker fulfilling the customer'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 licensees licensed from 1996 to 2009 and does not target a specifically named individual is excluded from the logging requirement.

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. *(Indicate what information should be captured in the log. Also identify the appropriate security controls for manual CPI logs, e.g., locked file cabinet.*)

D. Retention and destruction of a CPI log: [*Reference the agency’s record retention schedule to determine: a) the appropriate length for which CPI logs should be stored and b) the manner in which the logs should be destroyed*].

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 the *(add name of agency routine meeting, e.g., security or ethics)* meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing *(add name of system here)* which contains CPI.

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 *(agency)* policy.

8. Revision History

Date	**Description**
MM/DD/YYYY	New standard operating procedure

[Place on agency letterhead or procedure template]

(add Agency Name here)
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.		

[Place on agency letterhead or procedure template]

Template for "Incident Response for Access of Confidential or Sensitive Personally Identifiable Information for an Invalid Reason"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency. Make sure that it does not conflict with the agency's IT incident reporting procedure.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

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 *(add agency name here)* when Confidential Personal Information (CPI) or Sensitive Personally Identifiable Information (SPII) that is contained in a *(add agency name here)*-managed system is accessed for an invalid reason by a *(add agency name here)* 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 *(add and remove types of personally identifiable information to tailor the list to your agency)*:
    - 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 *(add agency name here)* has discretion not to release under public records law, and it also includes “confidential personal information,” which *(add agency name here)* is restricted or prohibited from releasing under Ohio’s public records law. Examples of “sensitive personally identifiable information” that *(add agency name here)* keeps includes *(add and remove types of SPII to tailor list to your agency)*:
    - 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
    - security challenge questions and answers
    - employees’ non-state-issued email addresses
    - medical and health information
    - fingerprints and other biometric information
    - driver’s license numbers
    - 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 *(add agency name here)* 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 *(add number of systems here)* personal information systems only:
    - *(Add system one)*
    - *(Add system two)*

- "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 *(add agency name here)* technology infrastructure, or to the threat of such an event.
- "Invalid reason" means any basis for access that is not directly related to *(add agency name here)* exercise of its powers or duties as described in the agency's CPI access policies. Ohio Administrative Code *(add rule reference here)*[1] identifies valid reasons for accessing CPI within the *(add agency name here)*.
- "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. <u>Response to access of CPI or SPII for an invalid reason</u>

   A. <u>Responsibilities.</u> *(Add agency name here)* employees and contractors have the following responsibilities when making a report of access of CPI or SPII for an invalid reason:

      a. <u>Employees</u> and <u>contractors</u> 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 DPPOC, Chief Legal Counsel or the Administrator for the program area involved.

      b. <u>Managers</u> or the party that received the initial report shall notify the agency Data Privacy Point of Contact (DPPOC) of the suspected incident at (add phone number here).

      c. The <u>DPPOC</u> shall notify the 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.

[1] *(Add URL for administrative rule here)*.

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;
- Agency Chief Legal Counsel; and
- Other parties as deemed appropriate.

d. If the review of the suspected incident determines that CPI or SPII has been inappropriately accessed, the Chief Legal Counsel shall report the incident in the following manner:

- Notify the *(Add agency name here)* 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 of the division involved 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 a *(add agency name here)* 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 *(add agency name here)* employee or contractor will provide no information and will direct the request to the *(add agency name here)* Communications Office, who will coordinate any public statements.

5. Training

A review of this procedure will be included on the agenda of the *(add name of agency routine meeting, e.g., security or ethics)* meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing any *(add agency name here)* 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 *(add agency name here)* policy.

7. Revision History

Date	**Description**
MM/DD/YYYY	New standard operating procedure

[Place on agency letterhead or procedure template]

Template for "Accessing Confidential Personal Information in a Paper-Based System"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

Standard Operating Procedure
Accessing Confidential Personal Information in a Paper-Based System
Insert office name here
Insert name of system here

---

1. Purpose
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add name of office here)* when accessing Confidential Personal Information contained in the paper-based system of record, *(add name of system here),* which is managed by the *(add name of office here)*.

2. Overview
   All state agencies, boards and commissions are required to implement Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of Ohio's citizens who have confidential personal information stored in a state-maintained, paper-based personal information system. The *(department name)* has issued administrative rules *(add citation to rules)* regulating access to confidential personal information. This procedure applies those rules to *(add system name here)*.

   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 III H of this procedure.

3. System Description
Note: Complete items A-I below. Add additional items as warranted to provide a full description of this system and the CPI that must be managed.

A. Name: *provide the name of the system here.*

B. Description: *provide a description of the system of record here.*

C. Purpose: *explain why this system is maintained and the purpose it serves.*

D. Regulatory requirements: *list the citation(s) (state or federal laws or rules) that require or support the existence and maintenance of this system.*

E. Authorizing access: *explain who authorizes access to the system, how those authorizations are maintained and how those authorizations are revoked when an employee terminates service or otherwise no longer needs access to CPI in the system.*

F. Security: *explain the security controls that exist with this system, such as locking mechanisms and the presence of authorized personnel.*

G. Positions that access the system:

Position title	Permission level (Full access, limited access, etc.)	CPI accessible with this permission level

H. Description of CPI Contained in this System: *Provide a list of the CPI contained in this system along with the federal or state statutes or administrative rules that make the confidential personal information confidential.*

I. Valid Reasons for Accessing CPI: *List the valid business reasons as to why this system is used. Be sure to also include the valid reasons for accessing CPI.*

4. 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*.

5. Training
A review of this procedure will be included on the agenda of the *(add name of agency routine meeting, e.g., security or ethics)* meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing *(add name of system here)* which contains CPI.

6. 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 *(agency)* policy.

[Place on agency letterhead or procedure template]

7. Revision History

Date	Description
MM/DD/YYYY	New standard operating procedure

[Place on agency letterhead or procedure template]

Template for "Accessing Sensitive Data"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

Standard Operating Procedure
Accessing Sensitive Data
Insert office name here
Insert name of system here

---

1. Purpose
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add office name here)* when accessing sensitive data contained in the *(add system name here)* which is managed by the *(add office name here)*.

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 *(add agency name here)* 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 *(add agency name here)* keeps may include *(add and remove types of sensitive personally identifiable information to tailor list to your agency)*:

- 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
- security challenge questions and answers
- employees' non-state-issued email addresses
- medical and health information
- fingerprints and other biometric information
- driver's license numbers
- state ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
- confidential personal information

3. System Description

   Note: Complete items A-I below. Add additional items as warranted to provide a full description of this system and the sensitive data that must be managed.

   A. Name: *provide the name of the system here.*

   B. Description: *provide the technical description of the system here, including the application used or the platform on which it resides.*

   C. Purpose: *explain why this system is maintained and the purpose it serves.*

   D. Regulatory requirements: *list the citation(s) (state or federal laws or rules) that require the existence and maintenance of this system.*

   E. Authorizing access: *explain who authorizes access to the system, how those authorizations are maintained and how those authorizations are revoked when an employee terminates service.*

   F. Security: *explain the security permissions that exist with this system such as passwords or other forms of authentication.*

   G. Positions that access the system:

Position title	Permission level (Full access, limited access, etc.)	Sensitive data accessible with this permission level

   H. Description of Sensitive Data Contained in this System: *Provide a list of the sensitive data contained in this system.*

   I. Valid Reasons for Accessing Sensitive Data: *List the valid business reasons as to why this system is used. Be sure to also include the valid reasons for accessing sensitive data.*

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 (insert policy number here), "Security Incident Response."*

5. Training

   A review of this procedure will be included on the agenda of the *(add name of agency routine meeting, e.g., security or ethics)* meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing the *(add system name here)* 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 *(insert agency name)* policy.

7. <u>Revision History</u>

Date	**Description**
MM/DD/YYYY	New standard operating procedure

[Place on agency letterhead or procedure template]

Template for "Request to Inspect Personal Information"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

Standard Operating Procedure
Request to Inspect Personal Information

---

1. Purpose
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add agency name here)* when responding to written requests to inspect Personal Information (PI) contained in a system managed by *(add agency name here)*.

2. Overview
   In accordance with Ohio Revised Code (ORC) 1347.08(A), upon the request of a properly identified person, every state agency that maintains a personal information system must:

   - inform that person of the existence of any personal information about him or her in the system;
   - permit the person to inspect that personal information in the system(s); and
   - inform the person about the types of uses made of the personal information and the identity of users granted accessed.

   Exceptions to ORC 1347.08 also exist and must be considered.

   ORC Section 1347.15(B)(5) requires state agencies to comply with a written request from an individual for a list of Confidential Personal Information (CPI) about the individual that the state agency keeps, unless the CPI relates to an investigation about the individual based upon specific statutory authority by the state agency.

   "Individual" means a natural person, an authorized representative, legal counsel, legal custodian or legal guardian of the individual.

"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. Some examples of personal 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
- timesheet

"Sensitive personally identifiable information" includes personally identifiable information that *(add agency name here)* has discretion not to release under public records law, and it also includes "confidential personal information," which *(add agency name here)* is restricted or prohibited from releasing under Ohio's public records law. Examples of "sensitive personally identifiable information" that *(add agency name here)* keeps includes *(add and remove types of sensitive personally identifiable information to tailor list to your agency)*:

- 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
- security challenge questions and answers
- employees' non-state-issued email addresses
- medical and health information
- fingerprints and other biometric information
- driver's license numbers
- 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 *(add agency name here)* 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 *(add number of systems here)* personal information systems only:

- *(add system name here)– (add division name here) (indicate whether system is computer-based or paper-based)*

3. <u>Requests to Inspect Personal Information</u>

   A. <u>Evaluate the Request</u>:

As a standard practice, general requests from individuals to review their own personal information should be routed to the appropriate *(add agency name here)* division records manager for evaluation. The requester must put the request for personal information in writing. Individual *(add agency name here)* offices may have specific business processes that involve the collection, verification or communication with customers regarding their personal information. This procedure does not supersede those business processes as long as those business processes are consistent with chapter 1347 of the Revised Code in providing individuals with an opportunity to review their personal information.

B. Verify the Identity of the Requester

If the personal information entirely constitutes a public record subject to disclosure under ORC 149.43, then it will be disclosed in accordance with *(add agency policy reference here)*. For personal information that is not a public record, however, the subject of the information still has a right, with some limitations, to review his or her own information under ORC Chapter 1347.

If the information requested constitutes sensitive personally identifiable information, then the law may give *(add agency name here)* the discretion in releasing the information to the public in general. If the personal information constitutes CPI, then the law prohibits the agency from releasing the information except to certain parties. *For this reason, the records manager must verify the identity of the requester of sensitive or confidential personal information to ensure that fulfilling the request for those types of personal information is appropriate.* To verify the requester's identity, the requester must appear in person and present a valid driver's license, official state identification card or passport. In the event an individual cannot present one of those three photo IDs, the department may accept a similarly trustworthy form of verification. Use of an alternative form of verification shall be approved by a deputy director prior to release the sensitive or confidential personal information.

C. Limitations on Disclosure

The records manager must notify the *(add agency legal office name here)* of each request for personal inspection of sensitive or confidential personal information. The records manager, in consultation with the *(add agency legal office name here)*, must determine if there are any requirements pertaining to the disclosure of the personal information or any legal restriction that limits the release of personal information to the subject of the information. Some examples include:

- *(Add agency name here)* is not required to release any confidential personal information under ORC 1347.15 that relates to an investigation about that individual.
- The records manager, in consultation with the *(add agency legal office name here)*, must disclose medical, psychiatric, or psychological information to a person who is the subject of the information or to the person's legal guardian, unless a physician, psychiatrist, or psychologist determines for the agency that the disclosure of the information is likely to have an adverse effect on the person. In this case, the information shall be released to a physician, psychiatrist, or psychologist who is designated by the person or by the person's legal guardian.
- *(Add agency name here)* must not release a confidential law enforcement investigatory record or trial preparation record as defined in divisions (A)(2) and (4) of section 149.43 of the Revised Code.

- *(Add agency name here)* is not required to release any personal information about an individual if the information is excluded from the scope of Chapter 1347 of the Revised Code.

D. Dispose the Request

Personal information is to be available for inspection during regular business hours, with the exception of published holidays. Personal information must be made available for inspection promptly. Copies of personal information must be made available within a reasonable period of time. “Prompt” and “reasonable” take into account the volume of personal information requested; the proximity of the location where the information is stored; and the necessity for any legal review of the information requested.

Each request should be evaluated for an estimated length of time required to gather the personal information. All requests for personal information must be satisfied within a reasonable time. Requests for personal information should be coordinated with the *(add agency communications office name here)* and the *(add agency legal office name here)*.

4. Costs for Personal Information.

Those seeking personal information will be charged only the actual cost of making copies.

- The standard charge for paper copies is 5 cents per page.
- The charge for computer files placed on a compact disc is $1 per disc.

Requesters may ask that records be mailed to them. Electronic sensitive personally identifiable information shall be sent to the requester in an encrypted format. The means of decrypting the information shall be sent through a separate communication. They will be charged the actual cost of the postage and mailing supplies. The office may require the requester to pay the cost of providing the information in advance.

5. Questions

For questions regarding this policy, please contact the *(add agency legal office name here)* at *(add phone number here)*.

6. Maintenance of this Procedure

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Sections 1347.08 and 1347.15 and with any corresponding *(add agency name here)* policy.

7. Revision History

Date	Description
MM/DD/YYYY	New standard operating procedure