State of Indiana Policy: *Information Privacy*

Version: 2.0 (8/2023)

Contents

1. Purpose

Indiana State Government believes in enabling the efficient and ethical use of data to drive decision making, protecting and respecting the privacy of Hoosiers while catalyzing innovation. Indiana's privacy program is unified under the State Chief Privacy Officer, which partners with State agencies to enable innovation and the adoption of emerging technologies while maintaining privacy as a core component of these initiatives. This unified approach fosters a culture that values privacy through the awareness of individual Hoosiers and the State employees who serve them.

The purpose of this Policy is to ensure that Personal Information maintained by the State of Indiana is processed in accordance with applicable law, regulation, and importantly, the expectations of Hoosiers.

2. Applicability

This Policy shall apply to all Personal Information as defined herein.

3. Revision History

Version	Date	Name	Revision Description	Supersedes
1	9/2017	T. Cotterill	Initial version.	n/a
1.1	6/2020	T. Cotterill	Adds reference to the State of Indiana Privacy Impact Assessment.	1.0
2.0	8/2023	T. Cotterill	Wholesale revision; greater alignment with Fair Information Practices Act.	1.1

4. Authority

This Policy is promulgated by the Office of the Chief Data Officer pursuant to Ind. Code Ch. 4-3-26. The OCDO may further promulgate component policies and/or subordinate standards, procedures, or guidance documents.

5. Ownership

Please direct questions and concerns to the following owner(s) of this Policy:

1. The State Chief Privacy Officer

6. Definitions

1. "APO" means the Agency Privacy Officer in each State Agency designated under this Policy.
2. "Fair Information Practices Act" or "FIPA" means the Act requiring state agencies to adhere to fair information practices and to respect the privacy of personal information, codified in Ind. Code Ch. 4-1-6.
3. "IOT" means the Indiana Office of Technology established by Ind. Code § 4-13.1-2-1.
4. "OCDO" means the Office of the Chief Data Officer established by Ind. Code § 4-3-26-9.
5. "PIA" means a privacy impact assessment as discussed herein.
6. "Personal Information" or "PI" has the meaning set forth in Ind. Code § 4-1-6-1(2).
7. "Policy" means this *State of Indiana Policy: Information Privacy*.
8. "Process" means any operation or set of operations performed, whether by manual or automated means, on Personal Information, such as the collection, use, storage, disclosure, analysis, deletion, or modification of Personal Information.
9. "State CPO" means the Chief Privacy Officer of the state.

7. Background

Through the daily operations of its agencies, the State of Indiana Processes vast amounts of information relating to its citizens and the governing process. This data is a valuable asset in providing government services to the public as well as informing the policymaking process to ensure the best outcomes for the Hoosiers we serve. Ensuring that Personal Information is Processed appropriately is of critical concern.

8. Policy

Maintaining the privacy of Personal Information is ultimately the responsibility of all State agency employees as they Process information in the course of their duties. To effectively maintain the privacy of Personal Information, State agency employees must understand the content of the Personal Information they process and how that content affects the agency's privacy obligations.

The OCDO seeks to establish a policy which enables State agencies to efficiently and ethically leverage Personal Information as they work on behalf of the Hoosiers we serve. To do so, the OCDO puts forth this Policy, which is adapted from *Best Practices: Elements of a Federal Privacy Program*, authored by the Federal CIO Council.[1]

The Policy includes six components, which are essential elements of an effective privacy management program. Those are leadership and accountability, privacy risk management and compliance documentation, privacy and data protection, incident response, notice and redress for individuals, and privacy awareness.

[1] *Best Practices: Elements of a Federal Privacy Program*, Federal CIO Council, (June, 2010), https://energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.

Each is discussed in greater detail below, framed in the context of the Indiana Fair Information Practices Act and our Indiana agencies' related legal obligations.

8.1. Leadership and Accountability

The State of Indiana's success in the maintenance of individual privacy begins with leadership. Information technology systems can be built to accommodate varying levels of access, but it is leadership that serves as the first step to ensure diligence on the part of State employees. To that end, this Policy establishes the role of the State Chief Privacy Officer. Created within the OCDO, the State CPO advises agencies on the application and enforcement of the Indiana Fair Information Practices Act, this Policy, its component policies, as well as subordinate standards, procedures, and guidance documents. In this capacity, the State CPO serves as counsel to agencies for internal, interagency, intergovernmental, and public-private efforts that involve Personal Information.

To further enable the development of privacy leadership within individual agencies, this Policy requires the designation of an Agency Privacy Officer in each agency. In most agencies, the APO is an as-needed role, and is most naturally suited to an attorney or technology leader with policy and program management abilities, creating alignment between day-to-day duties and the role of APO. The OCDO maintains a recommended job description for the APO, which is available on the Indiana Privacy Program webpage at on.IN.gov/privacy. The APO will work with the OCDO and will be responsible for the following:

- ensuring agency awareness of, and compliance with, applicable State and Federal privacy laws, regulations, and proposed revisions thereof;
- overseeing and coordinating agency privacy initiatives as described in this and related OCDO policies, standards, procedures, and guidance documents; and
- collaborating with other APO's and the State CPO, as necessary.

The APO must have a foundational understanding of the Fair Information Practices Act at Ind. Code Ch. 4-1-6, the Access to Public Records Act at Ind. Code Ch. 5-14-3, and any additional statutes and rules that govern Personal Information processed by the agency. The State CPO is available to assist APOs in the review and application of these and related statues and rules.

8.2. Privacy Risk Management and Compliance Documentation

As a multifaceted operation, the State of Indiana requires a heightened level of awareness from its subject-matter experts to ensure that Personal Information is Processed in a manner that respects the privacy of individuals. The APO must understand current and forthcoming agency efforts that may involve the Processing of Personal Information, ensuring the meaningful incorporation of privacy principles into the planning, design, development, deployment, operation, and monitoring of these initiatives.

8.2.1. Privacy Impact Assessments

On an annual basis, the APO will review an inventory of agency processes and systems to ascertain whether a PIA is required for each, in accordance with the *State of Indiana Standard: Privacy Impact Assessment Methodology: A NIST-Based Framework to Support Enhanced Privacy Protections within Government*. The APO will partner with

program and system owners to identify any new agency processes and systems that have been developed or procured that would require a PIA. For processes and systems that have previously been subject to the PIA process, the APO may require that another PIA be completed for that process or system.

If needed, the APO may partner with the State CPO to determine whether the PIA process is required in a given instance. The e-Government Act of 2002 offers general guidance as to when it is appropriate to conduct a PIA, particularly when significant changes are made to a system.[2] Significant changes to a process or system may include the following:

- New policies or procedures have been developed or implemented that affect how the process or system handles PI.
- Merging of the process or system's information with information from another process or system.
- Changes to the stakeholder management or ownership of the process or system.
- Modifications to the accessibility and information sharing processes of information in the process or system.
- Alterations to the character of the information in the process or system, such as the inclusion of new PI fields or changing previously anonymous information to PI.

8.2.2 Enterprise Data Catalog

At current, the OCDO is in the planning, design, and development phases of an enterprise data catalog for State Government. Following deployment, state agencies will be obligated to scan data Processing systems, capturing essential data source information in the process. With respect to the Indiana Privacy Program, this scan will include the following key attributes of scanned data sources, as required by *OCDO Standard: Indiana Privacy Program Data Classifications*:

- Automated decisionmaking questionnaire
- Granularity classification
- Privacy impact risk classification
- Security risk classification
- Records retention designation
- Regulatory classification
- Releasability questionnaire
- Storage location and trust questionnaire

Refer to the related standard via on.IN.gov/privacy for more information.

8.2.3 Information System Inventory

The APO will verify the annual submission of an information system report by the State agency as required by Ind. Code § 4-1-6-7. The information system report will be submitted using the mechanism(s) prescribed by relevant agencies. The information system report will, at a minimum, include the following:

1) The name or descriptive title of the information system and its location.

[2] Office of Management and Budget (2003, September 26). OMB guidance for implementing the privacy and provisions of the e-Government Act of 2002. https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf

2) The nature and purpose of the information system and the statutory or administrative authority for its establishment.
3) The categories of individuals on whom Personal Information is maintained, including the approximate number of all individuals on whom information is maintained and the categories of Personal Information generally maintained in the system, including identification of those which are stored in computer accessible records and those which are maintained manually.
4) All confidentiality requirements, specifically:
    (A) those information systems or parts thereof which are maintained on a confidential basis pursuant to a statute, contractual obligation, or rule; and
    (B) those information systems maintained on an unrestricted basis.
5) In the case of item (4)(A) above, the agency shall include detailed justification of the need for statutory or regulatory authority to maintain such information systems or parts thereof on a confidential basis.
6) The categories of sources of such Personal Information.
7) The agency's policies and practices regarding the implementation of Ind. Code § 4-1-6-2 relating to information storage, duration of retention of information, and elimination of information from the information system.
8) The uses made by the agency of Personal Information contained in the system.
9) The identity of agency personnel, other agencies, and persons or categories of persons to whom disclosures of Personal Information are made or to whom access to the system may be granted, together with the purposes therefor and the restriction, if any, on such disclosures and access, including any restrictions on redisclosure.
10) A listing identifying all forms used in the collection of Personal Information.
11) The name, title, business address, and telephone number of the person immediately responsible for bringing and keeping the system in compliance with the provisions of this chapter.

8.3 Privacy and Data Protection

Pursuant to Ind. Code Art. 4-13.1, the IOT has put forth the State of Indiana Information Security Framework, which provides requirements and direction to inform agency information security efforts.[3] Pursuant to Ind. Code Ch. 5-15-5.1, the Indiana Archives and Records Administration has put forth records retention schedules, which govern the retention and disposition of governmental records.[4] State agencies are expected to be in compliance with both the IOT's Information Security Framework and the Archives' records retention schedules, as they may apply. In context of this section of the Policy and in accordance with Ind. Code § 4-1-6-2, agencies must do the following:

1) Collect, maintain, and use only that Personal Information as is relevant and necessary to accomplish a statutory purpose of the agency.
2) Collect information to the greatest extent practicable from the data subject directly when the information may result in adverse determinations about an individual's rights, benefits and privileges under federal or state programs.

[3] https://www.in.gov/information-security-framework/.
[4] https://www.in.gov/iara/divisions/records-management/state-records-management/.

3) Collect no personal information concerning in any way the political or religious beliefs, affiliations and activities of an individual unless expressly authorized by law or by a rule promulgated by the oversight committee on public records pursuant to Ind Code. Ch. 4-22-2.
4) Assure that personal information maintained or disseminated from the system is, to the maximum extent possible, accurate, complete, timely, and relevant to the needs of the state agency.
5) Insofar as possible, segregate information of a confidential nature from that which is a disclosable public record and, pursuant to statutory authority, establish confidentiality requirements and appropriate access controls for all categories of Personal Information contained in the information system.
6) Maintain a list of all persons or organizations having regular access to Personal Information which is not a matter of disclosable public record in the information system.
7) Maintain a complete and accurate record of every access to Personal Information in a system which is not a matter of disclosable public record by any person or organization not having regular access authority.
8) Refrain from preparing lists of the names and addresses of individuals for commercial or charitable solicitation purposes except as expressly authorized by law or by a rule promulgated by the oversight committee on public records pursuant to Ind. Code Ch. 4-22-2.
9) Establish appropriate administrative, technical, and physical safeguards to insure the security of the information system and to protect against any anticipated threats or hazards to their security or integrity.
10) Exchange with other agencies official personal information that it has collected in the pursuit of statutory functions when:
    a. the information is requested for purposes authorized by law including a rule promulgated pursuant to Ind Code. Ch. 4-22-2;
    b. the data subject would reasonably be expected to benefit from the action for which information is requested;
    c. the exchange would eliminate an unnecessary and expensive duplication in data collection and would not tangibly, adversely affect the data subject; or
    d. the exchange of information would facilitate the submission of documentation required for various state agencies and departments to receive federal funding reimbursement for programs which are being administered by the agencies and departments.

8.3.1. Sharing Personal Information and Third-Party Risk Management

In the event an agency wishes to exchange Personal Information with a non-agency third party, the APO shall review the proposed data exchange to determine whether such an exchange is allowed under applicable law. If allowable, agencies shall use a data sharing agreement approved by the State CPO, in accordance with Ind. Code. § 4-1-6-8.6(a)(3). The State CPO can assist in these inquiries.

If legally feasible, the agency shall either: 1) conduct a third-party risk management assessment to evaluate the risk posture of the requestor's system proposed to host the Personal Information, ensuring that the requestor's system maintains sufficient controls to securely maintain the information in question; or 2) make the Personal Information available in an environment approved by the OCDO for this purpose. Details regarding the approved platform are available on the OCDO website at on.IN.gov/privacy. The Indiana Management Performance Hub

maintains environments approved by the OCDO for the exchange of Personal Information for analysis purposes and OCDO is available to assist agencies as they embark on their data sharing journey.

8.3.2. Data Publication: Suppression and Obfuscation

From time to time, state agencies make Personal Information available to the public. There is significant privacy risk in this process as individual data subjects can be directly identified or reidentified, even when data has been deidentified prior to publication.

Personal Information made available to the public must meet relevant obfuscation standards prior to its release. The OCDO is available to assist agencies with the data release process through the Indiana Management Performance Hub Data Review Team and OCDO Privacy Board. Reference *OCDO Guidance Document: Data Suppression and Obfuscation* for detailed suppression and obfuscation instructions. Visit on.IN.gov/privacy for more information.

8.3.3 Governance of Agency Analytics Environments

Pursuant to *State of Indiana Policy: Fair Information Practices related to Agency Analytics Environments*, state agencies may not utilize agency-managed analytics environments to enable the unrestricted interagency exchange of data. Such exchange is subject to this and other OCDO policies, standards, procedures, and guidance. Visit on.IN.gov/privacy for more information.

8.3.4 Cloud Service Providers and Privacy Risk Management

In the event an agency engages a cloud service provider for the Processing of Personal Information, the agency shall strive to create a verifiable trust-based relationship with the cloud service provider, in accordance with *IOT-CS-SEC-10, Cloud Product and Service Agreements*.

To achieve 'trust,' an agency shall, subject to policies and procedures of the IOT and the Dept. of Administration, incorporate into its contract with the provider the *State of Indiana Additional Terms and Conditions* relating to software, platform, or infrastructure as a service engagements, as appropriate.[5]

Verifiability is then enabled by incorporating into the contract robust continuous monitoring and regular independent audit obligations, providing an ongoing assurance that Personal Information under the stewardship of the cloud service provider is maintained in accordance with the *State of Indiana Additional Terms and Conditions* and applicable legal and regulatory requirements.

8.4 Incident Response

State agencies are expected to comply with Ind. Code Ch. 4-1-11 and related incident response policies put forth by the IOT. As applicable to state agencies, a breach is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency. Note that this Indiana Code chapter, governing notice of security breach by a state agency, uses a narrowly-tailored definition of personal information, when compared with the Fair Information Practice Act

[5] https://www.in.gov/idoa/state-purchasing/contract-administration/contract-forms-manuals-and-templates/.

definition used throughout this Policy. See Ind. Code § 4-1-11-3 for more information. In this context, a breach does not include the following:

1) Good faith acquisition of personal information by an agency or employee of the agency for purposes of the agency, if the personal information is not used or subject to further unauthorized disclosure.
2) Unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed.

Ind. Code § 4-1-11-2.

If such an event occurs, the IOT maintains the Indiana Security Incident Response Team ("ISIRT"), which must be immediately alerted via isirt@iot.IN.gov. The ISIRT will respond and require state agency action in accordance with Information Security Framework Standards *IOT-CS-SEC-133* and *IOT-CS-SEC-134*.

In the event of a breach of Personal Information, following any necessary mitigation, disclosure, and notification activities, the APO must provide to the State CPO documentation of actions taken.

8.5 Notice and Redress for Individuals

A well-rounded privacy policy provides for multiple independent verifications that the privacy of individuals is being maintained appropriately. It is on those lines that this Policy restates and reinforces that which the Indiana General Assembly has already put forth related to individual rights. Where a state agency holds title to the Personal Information in a system, the agency must provide a mechanism for an individual to obtain notice, challenge, correct, or explain information in that system about the individual. Should a correction or explanation about the Personal Information be added to the originating agency's system, that agency must notify other state agencies maintaining copies of the Personal Information to ensure that all records are updated accordingly.

In context of this section of the Policy and in accordance with Ind. Code § 4-1-6-2, agencies must do the following:

1) Inform any individual requested to disclose personal information whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, are likely to result from nondisclosure, whether the information will be treated as a matter of public record or as confidential information, and what rules of confidentiality will govern the information.
2) Make reasonable efforts to furnish prior notice to an individual before any personal information on such individual is made available to any person under compulsory legal process.

The State of Indiana's obligations with respect to notice for individuals is most evident in the circumstances where government and individuals interact with great frequency and ease. No means of interaction is more common than a State agency's presence on an internet gateway, or website. Due to their unique nature, and the frequency and ease with which the State of Indiana and individuals interact using the internet, government must provide notice to website users of its obligations under the Fair Information Practices Act and any other legal framework to which a particular agency may be subject.

As such, each agency maintaining a public-facing internet gateway, or website, shall provide a conspicuous link on all pages of that website to a privacy notice for individuals. The privacy notice displayed shall align with applicable legal frameworks, including Fair Information Practice Principles, and shall be approved by the State CPO.

State Agencies must also enable individuals to review Personal Information about them.

> Unless otherwise prohibited by law, any state agency that maintains a Personal Information system shall, upon request and proper identification of any data subject, or a data subject's authorized agent, grant the subject or agent the right to inspect and to receive at reasonable, standard charges for document search and duplication, in a form comprehensible to the subject or agent:
>
> (a) all Personal Information about the data subject, unless otherwise provided by statute, whether the information is a matter of public record or maintained on a confidential basis, except in the case of medical and psychological records, where the records shall, upon written authorization of the data subject, be given to a physician or psychologist designated by the data subject;
> (b) the nature and sources of the Personal Information, except where the confidentiality of the sources is required by statute; and
> (c) the names and addresses of any recipients, other than those with regular access authority, of Personal Information of a confidential nature about the data subject, and the date, nature, and purpose of the disclosure.

Ind. Code § 4-1-6-3.

> If the data subject gives notice that the data subject wishes to challenge, correct, or explain information about the data subject in the Personal Information system, the following minimum procedures shall be followed:
>
> (a) the agency maintaining the information system shall investigate and record the current status of that Personal Information;
>
> (b) if, after the investigation, the information is found to be incomplete, inaccurate, not pertinent, not timely or not necessary to be retained, it shall be promptly corrected or deleted;
>
> (c) if the investigation does not resolve the dispute, the data subject may file a statement of not more than two hundred (200) words setting forth the data subject's position;
>
> (d) whenever a statement of dispute is filed, the agency maintaining the data system shall supply any previous recipient with a copy of the statement and, in any subsequent dissemination or use of the information in question, clearly mark that it is disputed and supply the statement of the data subject along with the information;
>
> (e) the agency maintaining the information system shall clearly and conspicuously disclose to the data subject the data subject's rights to make a request;

> (f) following any correction or deletion of Personal Information the agency shall, at the request of the data subject, furnish to past recipients notification delivered to their last known address that the item has been deleted or corrected and shall require the recipients to acknowledge receipt of the notification and furnish the data subject the names and last known addresses of all past recipients of the uncorrected or undeleted information.

Ind. Code § 4-1-6-5.

8.6 Privacy Awareness

While the State of Indiana's success in the maintenance of individual privacy begins with leadership, all state employees must be aware of and assist with privacy-enhancing efforts.

In context of this section of the Policy and in accordance with Ind. Code § 4-1-6-2, agencies must do the following:

> Establish rules and procedures to assure compliance with this chapter and instruct each of its employees having any responsibility or function in the design, development, operation or maintenance of such system or use of any personal information contained in the system of each requirement of this chapter and of each rule and procedure adopted by the agency to assure compliance with this chapter.

Ind. Code § 4-1-6-2(11).

APOs are encouraged to educate employees of their agency regarding applicable privacy statutes and regulations. Interagency coordination by and between APOs is a core support mechanism to the State CPO in carrying out this Policy. The State CPO is available to assist APOs in their Processing initiatives, together catalyzing the State of Indiana's efforts to efficiently and ethically leverage Personal Information as we work on behalf of Hoosiers.

9. References

1. *Best Practices: Elements of a Federal Privacy Program*, Federal CIO Council, (June, 2010), https://energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.
2. Office of Management and Budget (2003, September 26). OMB guidance for implementing the privacy and provisions of the e-Government Act of 2002. https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf