OKLAHOMA
Office of Management
& Enterprise Services

Data Privacy Standard

Introduction

Exercising fair information practices to ensure appropriate treatment of personally identifiable information is critical to the information technology operations of the State of Oklahoma.

Additionally, OMES recognizes the importance of integrating privacy considerations into all aspects of state operations involving the use of technology and commits to the implementation of privacy by design principles.

Purpose

This document outlines the Fair Information Practice Principles and Privacy by Design principles all agencies must follow, as well as the requirement that agencies provide information to the OMES Information Services Cyber Command privacy team.

Definitions

Integrity – Guarding against improper information modification or destruction, which includes ensuring information non-repudiation and authenticity.

Personally identifiable information (PII) – Information which can identify an individual including, but not limited to, name, birth date, place of birth, mother's maiden name, biometric records, Social Security number, official state or government-issued driver license or identification number, alien registration number, government passport number, employer or taxpayer identification number or any other information that is linked or linkable to an individual, such as medical, educational, financial or employment information. This applies to any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means.

Standard

The FIPPs and Privacy by Design principles must be considered whenever a program or activity involving the use of technology raises privacy concerns or involves the electronic collection, processing, storage, access, dissemination or disposal of PII.

Agencies shall notify the OMES IS Cyber Command privacy team by opening a service ticket for privacy consultation before developing or procuring new technologies or systems that handle or collect PII, making significant modifications to such systems, or implementing or modifying processes in how PII is collected or handled.

The OMES IS Cyber Command privacy team may request information from any state agency relevant to the agency's implementation of the principles outlined in this standard. This may include but is not limited to requests for information and/or documentation needed for a Privacy Threshold Analysis, Privacy Impact Assessment, privacy investigation or other privacy concerns. All state agencies and staff will timely provide the OMES IS privacy team with accurate and complete information as requested.

<u>Fair Information Practice Principles (FIPPs)</u>

Agencies must follow the FIPPs outlined below to assure that the use of technologies sustains and does not erode privacy protections relating to the use, collection and disclosure of PII. Agencies use the FIPPs to assess and enhance privacy protections by analyzing the nature and purpose of the collection of PII to fulfill the agency's mission and how the agency

can best provide privacy protections in light of these principles.

The FIPPS are:

- Transparency – Agencies should be transparent and provide notice to the individual regarding the collection, use, dissemination and maintenance of PII.
- Individual participation – Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction and redress regarding the agency's use of PII.
- Purpose specification – Agencies should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- Data minimization – Agencies should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for the minimum time necessary to fulfill the specified purpose(s).
- Use limitation – Agencies should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the agency should be for a purpose compatible with the purpose for which the PII was collected.
- Data quality and integrity – Agencies should, to the extent practicable, ensure that PII is accurate, relevant, timely and complete.
- Security – Agencies should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification or unintended or inappropriate disclosure.
- Accountability and auditing – Agencies should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Privacy By Design principles.

Agencies shall take privacy into account as they design and deploy systems, products and services that affect individuals. In doing so, agencies must adhere to the following principles:

- Be proactive and preventative – Take proactive rather than reactive measures. Seek to anticipate and prevents privacy invasive events before they happen. Privacy by Design comes before-the-fact, not after.
- Privacy as the default setting – Seek to deliver the maximum degree of privacy by ensuring that PII is automatically protected in any given IT system or business practice. No action should be required on the part of the individual to protect their privacy − it should be built into the system, by default.
- Embed privacy into design – Embed privacy into the design and architecture of IT systems and business practices. Privacy is not an add-on, after the fact consideration − it should be an essential component of the core functionality being delivered and is integral to the system, without diminishing functionality.
- Full functionality/positive-sum – Seek to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.
- End-to-end security/full lifecycle protection – Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely

manner. Thus, Privacy by Design ensures cradle-to-grave, secure lifecycle management of information, end-to- end.

- Visibility and transparency – Assure all stakeholders that whatever the business practice or technology involved, it is in fact operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Trust but verify.
- Respect individual privacy – Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user-friendly options.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 51 O.S. §§ 151-172. OMES may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- U.S. Department of Homeland Security. (2008, December 29). *Privacy Policy Guidance Memorandum.*
- Cavoukian, Ann. (2011, January). *Privacy by Design: The 7 Foundational Principles*, Information & Privacy Commissioner of Ontario.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 08/29/2022	**Review cycle:** Annual
Last revised: 08/29/2022	**Last reviewed:** 01/29/2025
Approved by: Janet Morrow, Director of Risk, Assessment and Compliance	