State of Michigan
Administrative Guide to State Government

2610.01 Data Privacy

Issued: May 15, 2018
Revised: May 24, 2024

PURPOSE

Provide statewide privacy guidance to assist agencies with their implementation of an agency-specific privacy management program as prescribed in Executive Order 2016-24.

APPLICATION

This procedure applies to all Executive Branch Departments, Agencies, Vendors, Trusted Partners, Boards, or Commissions, including their employees, other agents (e.g. contractors), and temporary staff (herein after Users) who access or use state of Michigan (SOM) personal identifying information (PII), as defined in MCL 445.63.

This procedure is intended to be used as a general guide to agencies that collect PII and may or may not apply to an agency that merely handles PII previously collected by another agency (e.g. Records Management). It is not intended to replace or modify the advice or guidance of agency-specific legal counsel or an Agency's Privacy Protection Officer (PPO), who are the final authority in determining how to apply this guidance. In addition, each agency may have differing legal or regulatory requirements with respect to data that agency collects or maintains, and to the extent this procedure conflicts with applicable legal requirements, those legal requirements should always prevail. Note: regardless of whether an agency is subject to this procedure, they are still required to protect PII appropriately in accordance with applicable laws, policies, standards, or procedures.

All Users with access to PII must ensure its appropriate use as set forth in applicable laws or regulations, along with this and all SOM enterprise policies and procedures. PII is not limited to data in computing systems and is included wherever it resides, regardless of the form it takes (e.g. electronic, printed, etc.), the technology used to handle or store it, or the purposes it serves.

The Chief Data Officer (CDO) and Enterprise Information Management Steering Committee (EIMSC) are committed to protecting sensitive information. This procedure summarizes their strategic view of data privacy and offers a general guide to assist agencies in implementing this strategic view.

CONTACT AGENCY

Department of Technology, Management and Budget (DTMB)
Chief Data Officer (CDO)

Telephone: 517-243-7548

SUMMARY

Data privacy controls are designed to ensure the appropriate collection, use, and protection of citizens' PII. To protect citizen privacy, the CDO and EIMSC offer the following guidance. This guidance is patterned on the National Institute of Standards and Technology (NIST) Special Publication 800.53 Revision 5.

Using this guidance, along with any applicable legal or regulatory requirements, each agency should develop a strategy to comply with the framework, set forth in NIST 800.53. Agencies should refer to the most recent NIST 800.53 release for more information and a roadmap to implement effective privacy processes and management within the agency.

EIM Executive Order 2016-24 may be referenced for responsibilities of the CDO, PPO, and Chief Data Stewards. In addition, each Agency Director should consider their privacy responsibilities such as an overall agency privacy strategy, compliance posture, policies and procedures, and User awareness and training.

REFERENCES

Administrative Guide Policy 1305.00 Enterprise Information Technology (IT) Policy

Administrative Guide Policy 1340.00 Information Technology Information Security

Executive Order 2016-24

Michigan Identity Theft Protection Act (Act 452 of 2004)

Michigan Social Security Number Privacy Act (Act 454 of 2004)

NIST 800-53 Revision 5

SOM 1340.00.090.01.01 How to Handle a Security Breach Procedure

PRIVACY BUILDING BLOCKS

The following building blocks serve as a guide to the common themes among privacy controls and practices. Using these building blocks as a guide in conjunction with NIST resources may help an Agency establish minimum privacy controls. An Agency may elect even more stringent privacy controls if they choose, or they may be required to implement more stringent controls by applicable law or regulation.

Individual's Access to Their PII

For this procedure, an individual means the actual person, or authorized party (power of attorney, guardian, etc.) approved to act on their behalf in compliance with laws, rules, and regulations and/or at the discretion of the agency's PPO.

To the extent permitted by law, and where appropriate and reasonable, each agency should consider developing a process governing if and how individuals may request access to their PII for review, including how it may be corrected, updated, or disputed. The word "reasonable" as used in this procedure means something that does not cause a significant financial, time, or resource-related burden to the agency (at the discretion of the agency's PPO). If the agency chooses to provide a right of access to individuals to review their PII, we suggest applying the following guidance:

- Follow a documented process to permit access by an individual to their PII, if such access is reasonable and possible.
- The process should provide the individual with the following opportunities:
  - Review the accuracy and completeness of their PII;
  - Request copies of their PII;
  - Request in writing that any inaccurate PII be corrected, amended, or disputed, if reasonable and appropriate. The individual's written request should provide the reason and support for the requested correction or amendment, otherwise the requested change need not be considered. If an individual requests correction or amendment of disputed PII, and the agency denies such a request, the agency should provide the individual with a reason for the denial and an ability to challenge such denial unless a specific procedure and remedy already exists under state or federal law.
- The agency should have a process, and train users, to authenticate and verify the identity of an individual before granting access to or amending their PII.
- The agency should make clear that the right to change data may require the individual to file a court action, if for example an individual decides to challenge the contents of a recorded public record or a law enforcement file.
- The right to amend PII does not necessarily permit changes to a record or event that has actually occurred (such as investigative notes), even though PII should be factual to the extent possible.
- An agency should provide appropriate means of individual redress to ensure there is an effective way to have privacy concerns reviewed. An agency should establish or rely on existing procedures to receive and respond to complaints or inquiries about their procedures relating to the collection and subsequent handling of PII. The inquiry process should be easily accessible and simple to use. To the extent a concern or complaint is not adequately addressed, the agency should provide the ability for the individual to escalate the matter.

Transparency – Notice

To the extent permitted by law and where applicable, each agency that collects PII should inform employees and individuals about their privacy policies and procedures and describe the purposes for which PII is collected, used, maintained, and disclosed in its privacy notices.

- A privacy notice should contain (at a minimum) the authority to collect PII, a description of the information collected by the agency; the source of that information if not from the individuals themselves; a statement regarding the purposes for the PII collection; how the PII will be used; types of entities to whom the PII may be disclosed (if any); the individual's rights and choices (if any), as well as the consequences (if any) for not providing the information; and where the information is maintained.

- Notice should be provided in a timely manner (at the time or before the time PII is collected or as soon as practical afterwards), and hard copies should be provided to an individual upon request. Additionally, each agency should deliver notices to individuals as required by applicable laws, and in the appropriate accessible format. Where an agency collects PII from an individual, it should place its privacy notice on its website, if it has one.
- The notice should include language about how PII will be maintained, secured, and disposed of appropriately.
- The notice, or corresponding policies and procedures, should provide an individual the means to communicate with the appropriate person about privacy activities, including the notice, and any corresponding policies and procedures.
- Agencies should draft a notice using simple language.
- Agencies should review existing notices (in any format) and create new notices, as needed, to assure compliance with this procedure.
- The agency should maintain a record of what notices are given, when they are given, and to whom they are given; and maintain copies of all notice forms that are distributed.
- Notices should be clearly dated, and agencies should track previous iterations of their notice(s), policies and procedures, and documents that these changes are communicated to staff and individuals. An agency informs individuals of a change to a previously communicated privacy notice, for example, by posting notification on their website, sending written notice via postal mail, or email.

Transparency – Consent

To ensure compliance with the requirements of NIST 800.53, an agency that collects PII should provide individuals with permitted and appropriate choices over the collection, use and disclosure of their PII. The agency should also communicate the effects of those choices on the individual's ability to access the agency's services. An agency electing to collect PII should consider the following:

- Creating an agency-specific privacy notice as described above.
- Determining whether existing or new processes require consent, and if so, what consent is required to assure compliance with applicable laws.
- Best practice states PII collection and processing must be restricted to only that which is authorized by law. However, if legal authority does not exist – that is, the agency elects to collect PII but there is no legal requirement for that agency to do so - the agency should define what PII elements are being collected and for what purpose. Agencies collecting PII for any reason other than complying with a legal requirement should provide individuals with the ability to consent before collecting their PII.
- Before asking an individual to disclose their PII, the agency should inform the individual whether that disclosure is mandatory or voluntary, by what statute or other authority, and how that agency will use the PII.

- An agency collecting PII for non-investigatory or statutorily required purposes should allow individuals to revoke their consent to use their PII if an agency determines such a revocation is reasonable.
- Consent and accommodation are not generally required to collect PII where applicable laws impose obligations on the agency to collect it.

Program Planning, Management and Accountability

An agency that collects PII should define, document, communicate, and assign accountability for its privacy processes. Effective controls should also be in place either at a SOM enterprise or agency level for governance, planning, monitoring, and risk management to comply with applicable privacy protection requirements and to minimize risk.

- The Agency should name a PPO and identify individuals with privacy roles and responsibilities, including those tasks that require program planning and coordination (e.g., assessments, audits, system maintenance, testing, etc.).
- The Agency should develop a privacy strategy consistent with the agency mission and data in their care. Budgets, resource allocation plans, and oversight should be part of the strategy to address the privacy program needs.
- An Agency should have a strategy to review compliance with privacy policies, practices, controls, and procedures, and to comply with audits of privacy controls and monitor plans of action to address gaps in compliance.
- Each agency should develop a strategy to report to their leadership the overall status of their privacy program, including the status of meeting privacy requirements, metrics, complaints, or concerns.
- The Agency should follow an Information Privacy (or Security) Awareness and Training policy for employees who handle PII aimed at ensuring personnel understand privacy responsibilities and procedures. The Agency should ensure Users who handle PII are provided training under the authority for its collection and the procedures required to safeguard that information. This may be a combination of SOM enterprise-wide general privacy awareness and training, and agency targeted, role-based training.
- Each agency should maintain an inventory of systems that process PII.
- Each Agency should follow a process describing how systems containing PII operate (controls, architecture, and operational procedure) by conducting privacy and security assessments using the SOM Governance, Risk and Compliance tool and accreditation process.
- An Agency should follow a defined process when collecting and processing PII that minimizes the privacy risk to individuals. That process may include limiting the use of PII in testing, training, research, audit records, and visitor logs.
- An Agency should develop and/or follow existing privacy policies and ensure they are communicated and made available to all relevant parties.

- The Agency should determine which laws are applicable to their collected PII and monitor state and federal privacy laws, regulations, and policies for changes that may affect their programs.
- An Agency should develop and/or follow a documented incident management process, including but not limited to, specifying how an employee is to report a potential privacy incident; training to identify and respond to an incident; testing the incident response capability of systems; tracking and documenting incidents including any lessons learned and assessing any potential privacy harm to individuals. Agency specific plans should be coordinated with SOM 1340.00.090.01.01 How to Handle a Security Breach Procedure.
- An Agency should follow a process to classify PII.

AUTHORIZATION

Authority

The CDO is accountable to the EIMSC for identifying privacy best practices. The CDO has authority, along with this procedure, under:

- Executive Order (EO) 2016-24.
- MCL 18.1101, et seq.; MCL 18.41.
- The Administrative Guide to State Government.
- EO 2001-3, Creation of the Department of Technology, Management and Budget.
- Executive Reorganization Order (ERO) 2001-1, compiled at § 18.41 of the Michigan Compiled Laws (Management and Budget Act, PA 431 of 1984, Section 18, and ERO 2001-1 now contained in the Act, Section 18.41, Paragraph H).

***