2610.01 Data Privacy

Issued: May 15, 2018
Revised:

PURPOSE

To ensure agencies implement a privacy management program and processes to facilitate compliance with state and federal laws, regulations, policies, statutes, and rules 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 and other agents and temporary staff (hereafter Users) who access or use state of Michigan (SOM) personally identifiable data or potentially personally identifiable data (hereafter PPID). All Users with access to PPID shall ensure its appropriate use as set forth in this and all SOM enterprise policies and procedures. PPID is not limited to data in computing systems and is included wherever it resides in an agency, regardless of the form it takes (electronic, printed, etc.), the technology used to handle or store it, or the purposes it serves.

Adherence to this procedure, the privacy building blocks, and the recognized framework does not guarantee compliance with all laws and regulations. Agencies need to be aware of the significant privacy requirements that may apply to data in their care and consult their legal counsel for advice on laws and regulations governing the data in their care.

The Chief Data Officer (CDO) and Enterprise Information Management (EIM) Steering Committee (SC) are committed to protecting sensitive information. This policy summarizes their strategic view of data privacy.

CONTACT AGENCY

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

Telephone: 517-241-5545

Fax: 517-241-8715

SUMMARY

Data privacy controls are designed to ensure the appropriate collection, use, and protection of citizens' PPID. To protect citizen privacy, the CDO and EIMSC approved the privacy building blocks listed below. These building blocks are patterned after two nationally recognized privacy frameworks: the American Institute of Certified Public Accountants' Generally Accepted Privacy Principles (GAPP) and National Institute of Standards and Technology (NIST) Special Publication 800.53 rev 4, Appendix J.

Each Agency is to develop a plan to comply with this procedure and select a recognized privacy framework, such as GAPP or NIST, for additional privacy principles and supplemental controls. That framework will be a roadmap to implement effective privacy processes and management within the Agency and further evaluate and implement necessary privacy controls based on an Agency's mission and the data in their care.

PRIVACY BUILDING BLOCKS

The following building blocks embody various recognized privacy frameworks and identify common themes among privacy principles and practices. Using these building blocks, along with a detailed privacy framework, establishes the basis for an Agency to effectively implement baseline privacy controls. Within one year from the date of issuance of this policy, all SOM Agencies must adopt a documented privacy framework and develop an implementation plan addressing the following policy building blocks. The timeframe for achieving a fully defined and managed privacy program will be in accordance with each agency implementation plan.

Access

To the extent permitted by law, and where appropriate and reasonable, each Agency is advised to develop a process governing how individuals may request access to their PPID for review and how it may be corrected, updated or disputed.

Choice

To the extent permitted by law and where applicable, each Agency is advised to inform individuals about the choices available to them, if any, with respect to the collection, use, and disclosure of PPID, and where consent is required to disclose their PPID, unless a law specifically allows otherwise.

Notice

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

Security

Security in the context of data privacy means information security. Each Agency is advised to implement effective administrative, technical, and physical security controls appropriate to the sensitivity of the PPID to protect against loss, misuse, alteration, and unauthorized disclosure. The SOM addresses information security controls through Administrative Guide to State Government 1305.00 Enterprise Information Technology Policy; 1340.00 Information Technology Information Security Policy; and other applicable policies, standards, and procedures.

Management

Each Agency is advised to provide training to Users who handle PPID under the authority for its collection and the procedures required to safeguard that information. This should include any SOM enterprise-wide general privacy

awareness and training, and Agency targeted, role-based training for Users responsible for PPID.

Each Agency is advised to monitor state and federal privacy laws, regulations, and policies for changes that may affect privacy programs.

Each Agency is advised to follow a documented privacy incident and breach management procedure if they maintain PPID. Agency specific plans are to be coordinated with SOM 1340.00.090.01.01 How to Handle a Security Breach.

Each Agency is advised to provide oversight of their privacy processes, including a strategy to promote accountability and address potential gaps in privacy compliance.

ROLES AND RESPONSIBILITIES

Agency

Agency Director (or Designee)

- Establishes an overall strategy to develop and implement the Agency's privacy program based on this procedure and the privacy framework selected.
- Ensures internal Agency privacy policies and procedures are implemented and maintained to the extent necessary and properly enforced.
- Ensures Users are trained to handle PPID for which they are responsible in accordance with SOM and Agency policies and procedures and state and federal laws.

Privacy Protection Officers (or Agency Specified Equivalent)

- Coordinates Agency compliance with SOM enterprise-wide privacy policies and procedures and state and federal privacy laws.
- Advises Agency leadership on best practices for enterprise-wide privacy matters.

DTMB

DTMB Chief Data Officer (or Designee)

- Reviews and recommends SOM enterprise privacy policies and procedures.
- Identifies resources and provides guidance and best practices for privacy compliance.
- Serve as liaison to the Chief Data Stewards and Information Privacy Protection Officers on privacy-compliance issues.

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).

TERMS AND DEFINITIONS

The definition of terms is available in the Ad Guide Glossary (section 8000).

***