State of Michigan
Administrative Guide to State Government

2610.05 Management/Accountability

Issued: May 15, 2020
Revised:

PURPOSE

To ensure an Agency that collects potentially personally identifiable data (hereafter PPID) follows a privacy process addressing management and accountability.

APPLICATION

This procedure applies to all state of Michigan (SOM) Executive Branch Agencies who collect PPID. An Agency that collects PPID shall ensure its appropriate use as set forth in this and all SOM enterprise policies and procedures.

Adherence to this procedure does not guarantee compliance with all laws and regulations. An Agency should consult their legal counsel for advice on laws, regulations, other policies and procedures, specific business practices, contracts, or grants applicable to their data.

CONTACT AGENCY

Department of Technology, Management and Budget (DTMB)
Chief Data Officer (CDO)
Telephone: 517-241-5545 Fax: 517-241-8715

SUMMARY

An Agency that collects PPID defines, documents, communicates and assigns accountability for its privacy processes. Effective controls are also in place for governance, monitoring, and risk management in order to comply with applicable privacy protection requirements and to minimize risk.

PROCEDURES

1. Privacy policies are documented in writing, communicated and made available to staff (and third parties) who need them. Changes to policies and procedures are communicated shortly after approval.
2. The Agency follows an Information Privacy (or Security) Awareness and Training policy for employees who handle PPID aimed at ensuring personnel understand privacy responsibilities and procedures.
3. The Agency determines which laws are applicable to their PPID and monitors state and federal privacy laws, regulations, and policies for changes that may affect their programs.

4. An incident management policy is followed, including but not limited to, specifying how an employee is to report a potential privacy incident. An Agency may develop their own plan or rely entirely on SOM 1340.00.090.01.01 How to Handle a Security Breach.
5. A process is in place to classify PPID.
6. A process is in place to review compliance with privacy policies, practices, controls and procedures. The Agency complies with audits of privacy controls and monitors plans of action to address gaps in compliance.
7. A process is in place for privacy policies and procedures to be reviewed by agency legal counsel.
8. Risk management and assessment processes are in place to identify the risk to PPID.
9. A process is in place for Agency management and legal counsel to review contracts and Data Sharing Agreements involving PPID.
10. A documented information systems development and change management process is in place.

ROLES AND RESPONSIBILITIES

Agency

Agency Director (or Designee)

- Ensures that the Agency implements, maintains, and enforces internal Agency privacy policies and procedures consistent with enterprise-wide SOM privacy policies.

Privacy Protection Officers (also referred to as an Information Privacy Protection Officer (or Agency Specified Equivalent))

- Coordinates Agency compliance with this, and other, SOM enterprise-wide privacy policies and procedures and state and federal privacy laws.
- Coordinates work with appropriate business staff to develop and implement applicable Agency policies and procedures.

DTMB

DTMB Chief Data Officer (or Designee)

- Serve as liaison to the Chief Data Stewards and Privacy Protection Officers on privacy-compliance issues.

AUTHORIZATION

Authority

The CDO is accountable to the Enterprise Information Management Steering Committee for identifying privacy best practices. The CDO has authority, along with this procedure, under:

- Executive Order (EO) 2016-24.
- Administrative Guide to State Government 2610 Privacy Policy and 2610.01 Data Privacy Procedure.
- MCL 18.1101, et seq.; MCL 18.41.
- The Administrative Guide to State Government.

TERMS AND DEFINITIONS

Definition of terms available in the Admin Guide Glossary (section 8000).

***