State of Michigan
Administrative Guide to State Government

2610.06 Security (for Privacy)

Issued: June 2, 2020
Revised:

PURPOSE

Security in the context of data privacy means information security. The state of Michigan (SOM) and any supporting Agency privacy policies address the security of an individual's potentially personally identifiable data (hereafter PPID).

APPLICATION

This procedure applies to SOM Executive Branch Departments and 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. Agencies 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

To ensure administrative, technical, and physical security controls address the classification and sensitivity of the PPID collected to protect against loss, misuse, alteration, and unauthorized disclosure; and to preserve its privacy, confidentiality, integrity and availability.

This procedure acknowledges and defers to the suite of Information Technology security policies, standards and procedures already in place at the SOM.

PROCEDURES

1. Policies, standards and/or procedures address security measures used to safeguard PPID.
2. Security policies, standards or procedures exist for: encryption; awareness and training; authentication; data classification; physical security; risk assessment; access controls; network security; change management and patching; incident management; system integrity; disaster recovery and business continuity; portable media; storage; retention and disposal. Note: awareness and training programs include phishing safe practices.
3. Measures are in place to verify the identity of individuals that inquire about PPID whether they contact us in-person, or by phone, mail, or electronic mail.

4. Measures are in place to: detect threats to the network; identify potential environmental risk (e.g. flood, fire); address privacy and security protections in third party contracts.
5. An Agency addresses compliance with requirements established by Executive Orders, and federal and state laws or regulations pertaining to the confidentiality, integrity, availability and privacy of PPID.

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).

***