Subject: Handling of State of Michigan Sensitive Data and Information

Authoritative Policy: 1340 IT Information Security Policy

Procedure Number: TBD

Distribution: Statewide

Purpose: The public rightly assumes and should be assured that the data in the possession of Michigan state government is secure and protected from unauthorized disclosure. The objective of this document is to establish a statewide standard for protection of State of Michigan (SOM) sensitive information and data to help minimize the likelihood that such data is inadvertently or improperly disclosed.

Any user who has been authorized to access SOM sensitive information has an obligation to safeguard and protect the confidentiality of such data. It is the intent of this standard to provide guidance to management, staff and contractors as to their responsibility for the proper handling - production, processing, storage, transmission, and disposal of state sensitive information. Both physical and electronic data and information regardless of media type or means/method of disclosure (including information shared orally or visually – such as by telephone or video conference).

Handling is defined as the production, processing, access to, storage, transmission and disposal.

Contact/Owner: DTMB Michigan Cyber Security (MCS)

Scope: Executive Branch Departments and Sub-units, private partners and contractors.

Standard: State of Michigan Sensitive Information and Data (SOMSID) is defined as information whose handling or disclosure is protected, governed, mandated or restricted in some manner by federal or state statute or policy, rule, agreement or requirement. This data may also require protection for legal, ethical or procedural reasons, issues of personal privacy, or for proprietary considerations. The need to know for conducting official job responsibilities.

SOMSID includes, but is not limited data that must protected as defined in the following:

- Personal Information, as defined by the Michigan’ Identity Theft Protection ACT, ACT 452 of 2004
- Protected Health Information, as defined by the Health Insurance
Portability and Accountability Act of 1996 (HIPAA)
- Student education records, as defined by the Family Educational Rights and Privacy Act (FERPA)
- Card holder data, as defined by the Payment Card Industry (PCI) Data Security Standard
- Information that is deemed to be confidential in accordance with Internal Revenue Service
- Information that is deemed to be confidential by the Criminal Justice Information Service (CJIS)
- Information that is defined as sensitive by the agency.

Handling of SOMSID

Access or Use
1. Use of SOMSID must be approved by both:
   a. The system/data owner –and–
   b. The employee’s department head (or their designee)

   For non-SOM employees, “department” is defined as the SOM Agency contracting with the 3rd party.

2. The use of SOMSID’s must be restricted to individuals whose job duties require it. There must be a demonstrated need-to-know in support of conducting official SOM responsibilities.

3. ANY instance of SOMSID being lost, stolen, or where there is reasonable belief that an unauthorized person may have acquired or accessed the data; must be reported immediately. Refer to DTMB Standard 1340.00.01.02 “How to handle a breach of personal identifiable/sensitive information incidents” procedure.

4. Accesses to SOMSID must be protected in accordance with DTMB Standard 1335.00.02 “Authentication Requirements for Access to Networks, Systems, Computers, Databases, and Applications” standard. Applications Standard (former Ad Guide 1350.10)

5. Access to SOMSID must be logged and audited.

6. If SOMSID is accessed via a network a trusted connection. The Internet is not a trusted connection.

7. Access to SOM information systems by partners, and unauthorized external personnel must be restricted so that, in the event of an attempt to access SOMSID, the amount of information at risk is minimized. Connections may be set up to allow others (business partners, etc.) to see only what they need to see only when specifically authorized by the Business Owner.

Storage
1. SOMSID cannot be stored on privately-owned device.
2. SOMSID can only be stored on approved state-owned and DTMB
managed devices.
3. SOMSID must be encrypted at rest in accordance with DTMB Standard 1340.00.07 – Electronic Data Encryption.
4. The duration for which SOMSID can be stored on a (END USER) device must be granted for a finite duration as needed to fulfill the specific functions required to perform a specific job.
5. Storing SOMSID on “free” hosting sites such as DROPBOX is prohibited.

Transmission/Distribution
1. SOMSID must be encrypted in transit in accordance with DTMB Standard 1340.00.07 – Electronic Data Encryption. Examples:
   a. SOMSID cannot be stored on the state’s Office 365 SharePoint because data is not encrypted.
   b. SOMSID must not be transmitted via unsecure email. If SOMSID must be e-mailed, it must be encrypted and protected by a password. The password must be provided to the mail recipient(s) separately (e.g., by phone, another email, or in person).
   c. If SOMSID must be transmitted via USB thumb drive or other portable media, the drive must be secured and encrypted. Agencies are responsible for buying their own secured USB thumb drive from vendors approved by DTMB.
   d. SOMSID must be physically secure when in transit. Do not mail or courier SOMSID on CDs, DVDs, hard drives, USB flash drives, floppy disks, or other removable media unless the data are encrypted.

Disposal/Destruction
1. Do not return defective or failed hard drives to vendors for warranty repair or replacement if the device was ever used to store, process or access SOMSID.
2. Disposal and Destruction of data must be done in accordance with DTMB Procedure 1340.00.06 Storage of Sensitive Information on Mobile Devices and Portable Media.

Business Connections/Sharing
1. Data owners must have the necessary contract language, approved by the Attorney General to protect SOMSID if SOMSID is collected, used, processed, stored, or generated as the result of a service(s) not house in a SOM data center.
2. Sharing SOMSID via “free” hosting sites such as DROPBOX is prohibited.
Responsibilities

Management

All individuals having access to SOMSID are responsible for protecting SOMSID to the proper extent possible. All department heads or their designee are responsible for ensuring that their data is classified and that the classification activities are managed. If a manager is not certain of the classification to be applied, he or she should contact a higher level of authority (such as the Agency’s Director, Agency’s Legal Counsel, Internal Audit, State’s Chief Security Officer, or Attorney General, etc.).

Staff

If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager. If an employee feels that their manager is not following these standards, he or she should contact a higher level of authority (such as the Agency’s Director, Agency’s Legal Counsel, Internal Audit, State’s Chief Security Officer, or Attorney General, etc.).

Michigan Cyber Security

It is the responsibility of the Michigan Cyber Security liaison to provide guidance to all personnel on the use of these standards, and ensure that these guidelines are complied with. The liaison should report compliance related issues to the State’s Chief Security officer.

Penalties

Any employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment and/or criminal prosecution where the act constitutes a violation of law.

Any third party found to have violated this standard may be subject to action, up to and including criminal prosecution where the act constitutes a violation of law. A breach of contract and fiduciary liability may also apply.

Definitions:

Data/System Owner
Senior management of the Agency that is ultimately responsible of ensuring the protection and appropriate use of their business’ data.
Encryption
The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key that enables you to decrypt it.

Mobile Devices
Any mobile device (state-owned or privately-owned) capable of storing data. Examples include, but are not limited to: laptops, tablet PCs, Blackberrys, cell phones, PDAs, IPods, and players.

For the purpose of this standard, all non-state-owned computing or data storage equipment (e.g., PC, server, Network Attached Storage (NAS), and Storage Area Network (SAN)) are considered mobile devices.

Portable Media
Any portable media (state-owned or privately-owned) capable of storing data. Examples include, but are not limited to: external hard drives, USB thumb drives, flash drives, memory sticks and cards, CDs, DVDs, and floppy disks.

Approving Authority:

John Nixon, CPA
Director

Revised: TBD