

POLICY 1340.00 Information Technology Information Security

Issued: April 12, 2007

Revised: March 21, 2012

SUBJECT: Policy for Information Technology (IT) Information Security.

APPLICATION: This policy is intended for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using state of Michigan (SOM) information networks and IT resources.

PURPOSE: This policy establishes the SOM executive management strategic view of how information security shall be implemented to protect the SOM information from unauthorized access, use, disclosure, modification, destruction, or denial and to ensure confidentiality, integrity and availability of SOM information.

CONTACT AGENCY: Department of Technology, Management and Budget (DTMB)
Michigan Cyber Security

TELEPHONE: 517-241-4090

FAX: 517-241-2013

SUMMARY: All SOM employees, trusted partners, or any entity authorized to access the SOM information is obligated to protect the confidentiality, integrity and availability of the information as set forth in this and all SOM enterprise IT policies.

Information is not limited to data contained in computer systems but is inclusive regardless of where it resides within the agency, what form it takes, (*i.e.*, electronic, printed, etc.), what technology was used to handle it, or what purpose(s) it serves. This policy is based on three basic components of information Security for the purpose of this policy:

- **Confidentiality** – Limiting information access and disclosure to authorized users – “the right people” – and preventing access by or disclosure to unauthorized users – “the wrong people.” Confidentiality is defined as protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.
- **Integrity** – The trustworthiness of information resources. It includes the concept of “data integrity” – namely, that data have not been changed inappropriately, whether by accident or deliberate activity. It also includes the need to verify that the person or entity has entered the right information – that is, that the information reflects the actual circumstances and that under the same circumstances would generate identical data. Integrity is defined as guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.
- **Availability** – The availability of information resources. An information system that is not available when you need it is at least as bad as none at all. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure. Availability is defined as ensuring timely and reliable

access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Based on these three components of information security, any data that is originated, entered, processed, transmitted, stored or disposed of on behalf of the SOM is considered to be SOM information.

POLICY:

- Agency information is considered a SOM asset and must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification, destruction, or denial.
- Each agency Director is required to determine the proper levels of protection for their agency information and to implement the necessary safeguards.

Agency Director:

- As a Data Owner, the Director within their area of responsibility shall ensure:
 - Due diligence of confidentiality, integrity and availability of data.
 - Data management in compliance with Federal and state laws and regulations, and SOM policies.
 - Information security controls are implemented to protect the SOM information and that these controls are sufficient to ensure the confidentiality, integrity, availability of SOM information.
 - Information security controls are applied in a manner consistent with the value of the information.
 - Data business owner identification. Although it is not recommended to have multiple owners for the same data, this sometimes occurs. Where there is more than one owner, Data Owners must designate a Business Owner who will have authority to make decisions on behalf of all the owners of this data.
 - SOM agency information is identified and classified based on sensitivity, criticality and risk in compliance to Federal and state laws and regulations, includes a review at least once a year of the on-going need to continue protection, updates when the environment changes.
 - A system is established to identify baseline security controls to protect SOM information. Once it is identified and classified, ensure it is exposed only to those who have a need to know the information and a duty to protect it.
 - SOM agency information is safeguarded with the proper controls in accordance with its classification label.
 - Data, which is shared or transferred between agencies, is protected by the receiving agency with at least the same level of security used by the sending agency. The receiving agency assumes the responsibility of data owner for such data when it is transferred.
 - Anyone requiring access to confidential or restricted information that is owned by another agency must obtain permission from the Business Owner.
 - Controls are established to provide SOM oversight of trusted partners who handle SOM information on behalf of the SOM.
 - SOM agency information is disposed of and sanitized in compliance with SOM policies.
 - A formal internal process is established for reporting and responding to security breaches/incidents where there is reasonable belief that an unauthorized person may have acquired personal identifying information.

- A system is established to review technical controls and recommendations identified by the SOM data custodians.
- Internal agency security policies and procedures are implemented, maintained and enforced that compliment and comply with this policy.
- All SOM employees and trusted partners handle information for which they are responsible in compliance with this policy and all SOM IT policies.
- SOM employees and trusted partners are trained to ensure they are aware of their role in protecting SOM information and data as set forth in this policy.
- Employees are advised of the necessity of complying with DTMB policies and laws pertaining to the protection of SOM information, because non-compliance may leave the state liable and employees vulnerable to prosecution and civil suite, as well as disciplinary action.

DTMB Director:

- As a Data Custodian, the Director shall ensure:
 - Agencies are advised as to the best operational and technical controls necessary to protect their data in accordance with its classification label.
 - Agency-prescribed security controls and safeguards are implemented and monitored for compliance.

Terms and Definitions:

Agency	The principal department of state government as created by Executive Organization Act, P.A. 380 of 1965.
Availability	Ensuring timely and reliable access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.
Business Owner	Responsible for administration of systems is usually the owner of the primary business functions served by the application, the application's largest stakeholder.
Confidentiality	Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.
Data Custodian	An individual or organization that has responsibility delegated by a data owner for maintenance and technological management of data and systems.
Data/Information	SOM agency information. No distinctions between the words data and information are made for purposes of this policy.
Data Owner	An individual or organization – usually a member of senior management of an organization – who is ultimately responsible for ensuring the protection and use of data.
Due Care	Shows that an organization has taken responsibility for the activities that take place within the organization and has taken the necessary steps to help protect the SOM, its resources and employees from possible risk.
Due Diligence	The practice of implementing controls and safeguards that make sure the protection mechanisms are continually maintained and operational.

Information Technology (IT) Resources	Includes, but is not limited to: computers, servers, storage peripherals, telecommunications equipment, network equipment and wiring, network-attached printers and fax machines.
Integrity	Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.
Technical Policy(ies)	High-level executive management statements used to set directions in an organization that documents information values, protection responsibilities and management commitment for protecting its computing and information assets. Policies are strategic in nature.
Technical Standards	Published documents that contain technical specifications or other precise criteria designed to be used consistently as a rule, guideline or definition. They are also a collage of best practices and business cases specific to address an organization's technological needs. Standards are tactical in nature and derive their authority from a policy.
Technical Procedures	A series of prescribed steps followed in a definite order which ensure adherence to the standards and compliance as set forth in the Policy to which the Procedure applies. Procedures are operational in nature and derive their guidance from a standard and authority from a policy.
Trusted Partner/ Business Partner	A person (<i>i.e.</i> , vendor, contractor, 3rd party, etc.) or entity that has contracted with the SOM to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

Authority:

- This policy obtains its authority from:
 - Administrative Guide [Policy 1305 Enterprise Information Technology](#).
 - The [Administrative Guide to State Government](#).
 - DTMB [IT Technical Policies, Standards and Procedures](#), which can be found on the DTMB Intranet.

Enforcement:

- All enforcement for this policy shall be in compliance with the standards and procedures of Administrative Guide [Policy 1305 Enterprise Information Technology](#).

Developing Standards and Procedures for this Policy:

- All requirements for developing standards and procedures for this policy shall be in compliance with Administrative Guide [Policy 1305 Enterprise Information Technology](#).

Exceptions:

- All exception requests to this policy must be processed in compliance with Administrative Guide [Policy 1305 Enterprise Information Technology](#).

Effective Date:

- This policy will be effective upon signature of the Administrative Guide approval memo by the DTMB Director.
