POLICY 1305.00 Enterprise Information Technology (IT) Policy

Issued: April 12, 2007
Revised: July 12, 2019
Reviewed: February 9, 2021
Next Review Date: February 9, 2022

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

To establish statewide IT Policies, Standards and Procedures (PSP) and outline the authority, responsibility and oversight for ensuring enterprise IT PSPs are developed, implemented, maintained and enforced.

CONTACT AGENCY

Department of Technology, Management and Budget (DTMB)
Office of the Chief Technology Officer (CTO)

Telephone: 517-241-7681

Fax: 517-373-7268

SUMMARY

Develop, implement, and maintain a series of statewide IT PSPs that shall be adhered to.

IT policies (listed below) are located in the SOM Administrative Guide to State Government (Ad Guide); they include, but are not limited to, the following:

- IT Information Security Policy
- IT Network and Infrastructure Policy
- Project Management Methodology Policy
- Systems Engineering Methodology Policy
- IT Adoption, Acquisition, Development and Implementation Policy

Appropriate IT standards and procedures shall be developed, implemented and maintained under these high-level IT policies.

The SOM will base its IT governance framework on Control Objectives for Information Technologies (COBIT) (https://www.isaca.org/resources/cobit) and will select its IT security controls from and National Institute of Standards and Technology (NIST) (http://www.nist.gov/information-technology-portal.cfm) SP 800-53.

Protecting citizen information is a priority for Michigan. An enterprise IT policy approach is a solution geared toward establishing a statewide framework for IT PSPs to be used across the Executive Branch of state government.

Through this approach, enterprise PSPs are developed, implemented and maintained by the SOM for agency use. The result shall define the overall policy direction for SOM employees and business partners. With these guiding principles in hand, agencies may develop more stringent internal policies and procedures in cooperation with DTMB to protect their assets.

Agency Director

As a Data Owner, the Director within their area of responsibility shall ensure:

- Management, technical and operational controls are in place that protect the SOM and allow the SOM to satisfy its legal and ethical responsibility to protect the confidentiality, integrity and availability of the SOM's information.
- All employees are aware of DTMB and agency internal policies, standards and procedures to carry out these policies. They also need to understand the legal constraints within which they are to function.
- 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 suit.
- Internal agency policies and procedures are implemented, maintained and enforced that complement and comply with this policy.
- Agencies desiring to implement more stringent policies than those developed by DTMB may do so in conjunction with DTMB.

DTMB Director

As a Data Custodian, the Director shall ensure:

- A mechanism is in place to assist agencies with implementing the appropriate security controls to protect the agency's assets.
- A mechanism is in place that facilitates a statewide approach to IT PSPs.
- A mechanism is in place that helps to identify and prevent the compromise and misuse of the state's information, application, network and computers.
- A mechanism is in place to oversee and expand the use of project management principles.
- Enterprise IT PSPs necessary to facilitate the use of common technology across the Executive Branch of state government are developed and implemented.
- All agencies have access to the enterprise IT PSPs.

- A mechanism is in place to provide an enterprise approach for creation and maintenance of secure systems across the SOM network and infrastructure.
- A mechanism is in place to expand technological efficiencies related to common application development, customer support, risk assessments, shared data and greater citizen access, and expansion of network speed and capacity at a competitive cost.
- A mechanism is in place to facilitate a development and implementation process to replicate IT best practices.
- A mechanism is in place to develop service-level agreements with agencies.
- A mechanism is in place to monitor and evaluate new and emerging technology, which may be applicable for enterprise use, and determine the most effective way to introduce such technology into the current environment.
- A mechanism is in place to develop systems and methodologies to review, evaluate and prioritize existing and future IT projects.
- A mechanism is in place to acquire end user computing resources and services.

TERMS AND DEFINITIONS

Agency

The principal department of state government as created by the 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.

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.

Information Technology (IT)

Refers to software, hardware, networking, Internet of Things, and telecommunication products and services that the state uses to store, manage, access, communicate, send and receive information. IT also refers to data, voice and video technologies. The determination of whether something falls under IT is not dependent on cost (i.e., could be a free service) or whether the product or service is hosted on state systems.

Examples of IT products or services include, but are not limited to, the following:

- On-premise, commercial-off-the-shelf (COTS) software applications installed on state systems (e.g., Adobe Acrobat).
- Externally hosted, COTS software applications installed on a vendor's system (e.g., DocuSign, Salesforce, etc.).
- Custom developed software applications (e.g., DHHS' CHAMPS system).
- Software-as-a-Service (SAAS) applications hosted by a vendor (e.g., LexisNexis, Survey Monkey, etc.).
- Subscription-based information services (e.g., Gongwer, Gartner, etc.).
- Social media accounts (e.g., Twitter, Facebook, etc.).
- Mobile applications (e.g., iTunes).
- Server hardware and software used to support applications such as database, application/web servers, storage systems, and other hosting services (e.g., Dell EMC PowerEdge Blade server).
- Hardware devices (e.g., laptops, tablets, smartphones, etc.).
- Data, voice, and video networks and associated communications equipment and software (e.g., Cisco routers and switches).
- Peripherals directly connected to computer information systems (e.g., Ricoh scan printers, printers).
- Internet of Things (IOT) are objects with electronic components that include processing and networking capabilities designed to enhance the functionality of the object by leveraging communications over the internet (e.g., ADT Security, smart thermostat, software-enabled lab equipment, refrigerator with an LCD screen, etc.).
- Vendor services for software application, installation, configuration, development and maintenance, including staff augmentation arrangements (e.g., CNSI resources assisting with maintenance and support of the DHHS CHAMPS system).

To utilize or source a product or service that includes components that meet the definition of Information Technology, the agency shall engage with the designated General Manager, or Business Relationship Manager for consultation on the need for DTMB IT services, (e.g., Cyber Security, Agency Services, Enterprise Architecture, Telecom, etc.).

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. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention.

Technical Policy

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 Standard

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 Procedure

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

A person (i.e., vendor, contractor, third 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.

AUTHORIZATION

Authority

- Executive Order No. 2001-3, Creation of the Department of Technology (DIT).
- Executive Reorganization Order (ERO) No. 2001-1, compiled at § 18.41 of the Michigan Compiled Laws (Management and Budget Act 431 of 1984, Section 18, and ERO 2001-1 now contained in the Act, Section 18.121).
- Executive Reorganization Order (ERO) No. 2009-39, compiled at § 18.441 of the Michigan Compiled Laws (MCL), Paragraph F.
- This policy obtains its authority from Executive Order No. 2001-3. The enterprise IT PSPs developed under this "1305 Enterprise Information Technology" policy set forth the Department's position on a given subject. IT standards and procedures cannot override the authority of any IT policy.
- Public Act 389 of 2018, incorporated into PA 431 section 18.123 and 18.124 appointment and duties of Chief Information Officer (CIO).
- Public Act 389, Section 115, effective December 19, 2018 (http://www.legislature.mi.gov/documents/2017-2018/publicact/pdf/2018-PA-0389.pdf).
- The "1305 Enterprise Information Technology" policy is the mechanism used for establishing an enterprise approach to IT management and serves as the overarching umbrella policy for protecting the SOM information and assets. This policy and its supporting Ad Guide policies should be considered collectively rather than as separate or unrelated.

- Therefore, in order to ensure a consistent implementation of IT practices, the IT policies developed in the Ad Guide under “1305 Enterprise Information Technology” require mandatory compliance by all state agencies. The enterprise standards and procedures developed from these policies obtain its authority from the enterprise policies and are therefore mandatory as well.

Enforcement

- Any employee found to have violated this policy 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 SOM partner found to have violated this policy 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.

Developing IT PSPs

- A revision to a policy, standard or procedure may be necessary and the Director of DTMB shall be responsible for implementing a mechanism to determine when the need to write or revise a policy, standard or procedure is warranted.
- All SOM IT PSPs shall be reviewed and updated at a minimum of every five (5) years or more frequently, as required, to meet regulatory requirements [e.g., federal, state, Payment Card Industry (PCI), Criminal Justice Information System (CJIS), Health Insurance Portability and Accountability Act (HIPAA), personal identifiable information (PII), National Institute of Standards and Technology (NIST), etc.] that govern each policy. Revisions must be implemented within one year of updates.

Exceptions

- An exception to this policy directive shall be signed by the requesting agency Director, authorized by the DTMB Chief Information Officer (CIO), and granted only by the DTMB Director. Complete details for submitting and obtaining an exception can be found in the standards and procedures for this policy.

Effective Date

- This policy will be effective upon signature of the Administrative Guide approval memo by the DTMB Director, unless a future effective date has been specified.

***