

**POLICY 1325 Information Technology Security Awareness**

Issued: April 12, 2007

Revised: March 21, 2012

- SUBJECT:** Policy for Information Technology (IT) Security Awareness.
- 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 a statewide policy for the purpose of security awareness and training and to inform all levels of state personnel of the importance of the information they handle and the legal and business reasons for maintaining confidentiality, availability and integrity. All employees must understand the need for security, the specific security-related requirements expected of them, and the consequences of noncompliance.
- CONTACT AGENCY:** Department of Technology, Management and Budget (DTMB)  
Michigan Cyber Security
- TELEPHONE:** 517-241-4090
- FAX:** 517-241-2013
- SUMMARY:** This policy will address two major security awareness components:
- **Awareness (What)** – Identify and implement programs and products designed to convey general security information to SOM users. Such activities include, but are not limited to, a statewide information security awareness training program, generating security literature and promoting good security through security web sites and newsletters.
  - **Training (How)** – Identify and implement security training programs more specific to the user role (*i.e.*, project manager, system administrator, security liaison, etc.) within the agency. This will provide the users with training applicable to their level of responsibility.

**POLICY:**

- It is the agency/department who gathers data, enters it into the system, verifies its accuracy, specifies the purposes to which it can or will be used, designates who can use it, and ultimately fills a business need for its use.

**Agency Director:**

- As a Data Owner, the Director within their area of responsibility shall ensure:
  - The appointment of a security awareness coordinator who will serve as liaison to the DTMB security awareness coordinator.
  - All SOM employees and trusted partners complete the SOM Information Security Awareness training prior to accessing the SOM network and IT resources.
  - All SOM employees and trusted partners handle information for which they are responsible in a manner in accordance with this and all SOM 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.

- Internal agency security policies and procedures are implemented, maintained and enforced that compliment and comply with 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 suit, as well as disciplinary action.
- As a Data Custodian, in conjunction with the DTMB Chief Information Security Officer (CISO) shall ensure:
  - A structured SOM security awareness program is formulated and maintained to ensure that SOM employees and trusted partners who require access to the state's information in the conduct of official business are familiar with their responsibilities for protecting such information from unauthorized disclosure.
  - All agencies implement security awareness workshops for agency security awareness coordinators.

DTMB CISO:

- Shall ensure:
  - A security awareness coordinator is appointed to develop and implement an enterprise security awareness program.

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.
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.

\*\*\*