AUTH.01: MEDC Enterprise Information Technology Policy
Michigan Economic Development Corporation
Information Technology

Topic Area: Policy for Michigan Economic Development Corporation (MEDC) that assigns Information Technology (IT) authority over Policies, Standards, and Procedures that govern the use of technology for MEDC.

Application: This policy is intended for MEDC compliance and applies to all employees and trusted partners using MEDC information networks and IT resources.

Purpose: To establish MEDC IT Policies, Standards and Procedures (PSPs) and outline the authority, responsibility, and oversight for ensuring MEDC Information Technology PSPs are developed, implemented, maintained and enforced.

Contact/Owner: Michigan Economic Development Corporation
Information Technology

Telephone: (517) 373-8600

Fax: (517) 241-8797

Summary: Develop, implement, and maintain a series of MEDC IT PSPs that are adhered to.

IT policies (listed below) are published on the MEDC intranet; they include, but are not limited to, the following:

Security Awareness Policy

Access Control Policy

IT Information Security Policy

Network and Infrastructure Policy

Project Management Methodology Policy

Application Development Policy

Continuity of Business Planning Policy

Appropriate IT standards and procedures are developed, implemented, and maintained under these high level IT policies.

Additionally, the adoption of Control Objectives for Information and Related Technology (COBIT) concepts, the guidance and principles from International Organization for Standardization ISO 27002, and National Institute of Standards and Technology (NIST) best practices will be used as guidelines but not strictly adhered to. The MEDC PSPs represent the agreed upon guidelines for the organization.

Issued Date:	Last Revision:	Last Reviewed:	Next Review Date:
November 17, 2016	April 18, 2018	April 18,2018	April 18, 2019

Policy:

Protecting MEDC information is a priority for the MEDC IT unit. An enterprise IT policy approach is a solution geared toward establishing a framework for IT PSPs to be used across the MEDC.

Through this approach, MEDC’s PSPs are developed, implemented, and maintained by the Information Technology Unit for MEDC’s use. The result defines the overall policy direction for: state employees; corporate employees; trusted partners; and those select individuals allowed user access and privileges to conduct MEDC business on a short term and/or contingency basis. With these guiding principles, business units requiring more stringent internal policies and procedures must work in cooperation with IT to ensure that their specific data and technology assets are properly protected.

MEDC Staff:

As a Data Owner within his/her area of responsibility, each Staff Associate ensures that:

- Managerial, technical and operational controls are in place that protect their unit’s data within the MEDC, and allow the MEDC to satisfy its legal and ethical responsibility to protect the confidentiality, integrity and availability of MEDC’s information.
- They, individually, are aware of MEDC and the business unit’s internal policies, standards, and procedures and they are to carry out these policies. They also need to understand the legal constraints within which they are to function.
- They, individually, are aware of the necessity of complying with MEDC policies and laws pertaining to the protection of MEDC information because non-compliance may leave MEDC and/or the state liable and employees vulnerable to prosecution and civil suit.
- Internal business unit policies and procedures that are implemented, maintained, and enforced that pertain to the use of technology must comply with this policy.
- Business units desiring to implement more stringent policies than those developed by MEDC IT must do so in conjunction with MEDC IT.

MEDC CIO:

As a Data Custodian, the CIO shall ensure that:

- A mechanism is in place to assist the business units with implementing the appropriate security controls to protect the business unit assets.
- A mechanism is in place that facilitates an MEDC approach to IT PSPs.

- A mechanism is in place that helps to identify and prevent the compromise and misuse of the MEDC's information, application, network, and computers.
- MEDC IT PSPs necessary to facilitate the use of common technology across the MEDC are developed and implemented.
- All business units 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 MEDC 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 lower 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 the business units.
- 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:

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 Unit: A unit of organization with the MEDC.

Confidentiality: Protecting information from unauthorized disclosure or interception 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: MEDC information. No distinction between the words data and information are made for purposes of this policy.

Data Owner: An individual or business unit who is ultimately responsible for ensuring the protection, use and accuracy of data.

Enterprise: MEDC wide.

Information Technology (IT) Resources: Includes, but is not limited to, devices, networks, data, software, hardware, email, system accounts, and facilities provided to conduct official MEDC business.

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(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: A person (i.e., vendor, contractor, third party, etc.) or entity that has contracted with the MEDC to perform a certain service or provide a certain product in exchange for valuable consideration: monetary, or goods and services.

Authority:

- Executive Order No. 1999-1, formation of the MEDC.
- Executive Order No. 1999-1 and assigning IT Staff to the MEDC for the purpose of the administration of MEDC technology usage.
- The *AUTH.01: MEDC Enterprise Information Technology Policy* is the mechanism for establishing an enterprise approach to IT management and serves as the overarching umbrella policy for MEDC information and IT assets.

Enforcement: Any MEDC 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 MEDC Trusted 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.

Exceptions: Exceptions to any IT PSP can be requested through the IT Helpdesk. All exception requests will go through the normal PSP change procedure. The Requestor will be asked to explain their request at a meeting of the Cross Functional Review Team meeting.

Effective Date: November 17, 2016

Signature and Title of Approver:	**Date:**
Tilak Mohan, Chief Information Officer Digitally signed by Tilak Mohan DN: cn=Tilak Mohan, o=Michigan Economic Development Corporation, ou=Information Services, email=mohant1@michigan.org, c=US Date: 2018.04.17 08:36:02 -04'00'	April 18, 2018

Author:	Approver:	Approval Date:	Description of Change(s):
Kim Fedewa	Tilak Mohan	November 17, 2016	Original copy approval.
Kim Fedewa	TIlak Mohan	March 22, 2017	Modify Policy list in Summary section. Scale back strict adherence to NIST best practices to use as appropriate.
Kim Fedewa	Tilak Mohan	April, 18, 2018	Application: Abbreviated MEDC, added Trusted Partners. Policy: Added Trusted Partners. Terms and Definitions: Added Trusted Partners. Enforcement: Added Trusted Partners.