PMP.01: MEDC Enterprise Business Application Services Project Management Process Policy

Michigan Economic Development Corporation Information Technology

Topic Area: Policy for Michigan Economic Development Corporation Business Application Services (BAS) Project Management Process.

Application: This policy is intended for Michigan Economic Development Corporation (MEDC) compliance and applies to all MEDC, Boards or Commissions using MEDC Information Technology (IT) resources.

Purpose: This policy provides guidance for the development, enhancement and maintenance of new and existing IT systems with the MEDC.

Contact /Owner: Michigan Economic Development Corporation
Information Technology

Telephone: (517) 373-8600

Fax: (517) 241-8797

Summary: The intent of this policy is to document the best practices that promote the development, enhancement and maintenance of reliable, cost-effective, computer-based solutions. Information systems play an essential role in delivering a variety of services to MEDC's customers. The partnership between MEDC and its client business unit's results in high quality and cost effective automated solutions.

The BAS Project Management Process was created to assist the MEDC IT department in developing, enhancing and maintaining computer-based systems by establishing a consistent, structured project process.

This process provides guidance for MEDC BAS managers and staff, including contracted resources, as well as MEDC business unit managers and staff that function as partners with MEDC BAS. This process is sufficiently flexible to cover both new projects and maintenance activities of all sizes.

Policy: MEDC BAS and its client business units are required to follow the BAS Project Management Process for all IT projects.

Business Systems Management: As a System Owner, the Manager within their area of responsibility shall ensure:

- Alignment to business unit goals.
- Availability of sufficient and knowledgeable resources, including subject matter experts (SME), testers, policy experts and trainers.

Issued Date:	Last Revision:	Last Reviewed:	Next Review Date:
January 31, 2018	January 31, 2018	January 31, 2018	January 31, 2019

- Availability of resources authorized to test, approve and accept project deliverables.
- A mechanism is in place to collect, track and mitigate and/or resolve application and hardware vulnerabilities.
- Appropriate problem resolution has occurred and system issues are addressed and communicated accordingly.
- Business units are provided appropriate levels of technical support for ongoing operations.
- Coordination and communication of all changes to the project/system to all stakeholders.
- MEDC Staff and client business unit managers and staff are educated in BAS Project Management Process workflow.
- Availability of individual(s) to act as application system owner(s). An application system owner has ultimate responsibility for a system and is responsible for gathering information and providing management recommendations on the resources required to meet operational objectives. It is understood that no one person can know all the details of a system and its operations. Therefore some of the following responsibilities may be delegated to the teams reporting to the Business Systems Support, Manager:
    - Learn and understand the overall purpose of the system.
    - Learn and understand sufficient details of the system to be able to manage the day-to-day business operations of the system.
    - Make final decisions in situations where system information is inaccurate after appraising the customer impact as well as the resources and time available.
    - Provide final approval for implementation for all changes to the system.
    - Recommend improvements to the system to maintain an efficient and accurate business process providing customer oriented information.
    - Develop and maintain a system business continuity plan.
    - Conduct periodic review of the system operations to ensure they are working as intended.
    - Coordinate periodic reviews to ensure acceptable levels of documentation –including audits and controls to ensure data integrity – and procedures for operating and maintaining the system.

- Develop specifications for what the system will and will not do (including reporting).
- Ensure there are polices and processes for granting access to the system and a process for periodic review of the access.
- Oversee the administration of training development and presentation for all staff that will update or use the information in the system.
- Ensure applications are secure; that personal and confidential data is protected; and that risk assessment is completed to identify vulnerabilities in the system.

MEDC Chief Information Officer (CIO):

- As the position for overseeing the system development, the CIO shall ensure:
- Business units are provided with a governance team:
  - To which project and operational metrics are provided.
  - Through which decisions about the project or system – escalated issues – can be resolved.
- Business units are provided information and recommendations about the best technical approaches to meet business needs.
- Business units are provided reliable and cost-effective technical solutions by researching the applicability of commercial off the shelf solutions and other shared IT solutions.
- A mechanism is in place to collect, track and mitigate and/or resolve application and hardware vulnerabilities.
- Appropriate problem resolution has occurred and that system issues are addressed and communicated accordingly.
- Business units are provided appropriate levels of technical support for ongoing operations.
- Coordination and communication of all changes to the project/system to all stakeholders.
- MEDC staff and client business unit managers and staff are educated in BAS PMP process workflow.
- Projects are resourced correctly with:
  - Project managers commensurate with the project size, complexity and importance.
  - Team members that are skilled or adequately trained in the technologies used.
  - Appropriate tools to complete the assigned tasks.

- Application development standards that maintain data integrity and security are developed, maintained and followed.
- An IT disaster recovery plan – fulfilling the business unit funded "recovery time objective" and the "recovery point objectives" – is recommended, developed and maintained.
- All third-party provided IT resources are managed to afford the MEDC the best value for the contractual cost.

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 within the MEDC.

Confidentiality: Protecting information from unauthorized disclosure or interception assuring that information is shared only among authorized persons and organizations.

Data/Information: MEDC information. No distinction between the words data and information are made for purposes of this policy.

Data Owner: A business Unit who is ultimately responsible for ensuring the protection, use and accuracy 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 MEDC, its resources and employees from possible risk.

Due Diligence: The practice of implementing controls and safeguards that insure protection mechanisms are continually maintained and operational.

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.

Formal Project Management Practices: Using formal practices and procedures within the MEDC Project Management Methodologies to manage a project.

Methodology: A system of principles, practices and procedures applied to a specific branch of knowledge. A documented approach for performing activities in a coherent, consistent, accountable and repeatable manner.

System Owner: From an enterprise perspective, the unit that funds and has approval authority for a project. From an application perspective, individual(s) that has ultimate responsibility for a system and is responsible for gathering information and providing management recommendations on the resources required to meet operational objectives.

Template: Templates establish the initial document setting and formats. A word processing program like Microsoft Word uses the "normal" template as the basis for all documents. A user can modify the "normal" document and/or create other templates to use.

Trusted Partner/Business 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 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 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.

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: March 15, 2017

Signature and Title of Approver:	**Date:**
Tilak Mohan, Chief Information Officer	March 15, 2017

Author:	Approver:	Approval Date:	Description of Change(s):
Patricia Blogg	Tilak Mohan	March 15, 2017	Original copy approval.