MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	**MICHIGAN ECONOMIC DEVELOPMENT CORPORATION** Information Technology	**Standard:** **SECU.01.070.01**
Topic Area:	**Contingency Planning Standard**	
Distribution:	**All Michigan Economic Development Corporation Staff**	

Purpose: To define the Contingency Planning security controls for Michigan Economic Development Corporation (MEDC) information systems. This standard aligns with National Institute of Standards and Technology (NIST) security framework 800-53, Revision 4, Contingency Planning (CP).

Contact/Owner: Michigan Economic Development Corporation
Information Technology

Scope: This standard is applicable to all information systems that are part of the MEDC, Boards or Commissions, and business or vendor partners that manage MEDC Information Technology (IT) resources including, but not limited to, networks, systems, computers, data, databases and applications.

Standard:

INTRODUCTION

This document defines the security control baseline for MEDC information systems as they relate to Contingency Planning. All security controls listed in this document, (e.g., software, hardware, performance, functional, infrastructure, etc.) must be used to evaluate MEDC IT systems and be included in the requirements for purchasing or building new systems.

The MEDC has adopted a Moderate baseline set of security controls identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) from the NIST Computer Security Resource Center (http://csrc.nist.gov/publications/PubsSPs.html). The detailed controls below for Contingency Planning have been taken directly from NIST Special Publication 800-53 and have been modified in some cases for MEDC implementation.

This standard dictates the Contingency Planning security controls for every MEDC information system. These are identified as the MEDC minimum Contingency Planning baseline. Business units, based on their business programs, may need to be compliant with additional security requirements (e.g., Payment Card Industry (PCI) security requirements, Internal Revenue Service (IRS) security requirements, or Criminal Justice

Issued Date:	Last Revision:	Last Reviewed:	Next Review Date:
September 19, 2018	September 19, 2018	September 19, 2018	September 19, 2019

Information System (CJIS) security requirements) and should comply accordingly.

THE CONTROLS

CP-2 Contingency Plan

MEDC IT, along with the system and/or data owner where applicable, will ensure that the following baseline controls are implemented and documented:

- Develops a contingency plan for the information system that:
  - Identifies essential missions and business functions and associated contingency requirements.
  - Provides recovery objectives, restoration priorities, and metrics.
  - Addresses contingency roles, responsibilities, assigned individuals with contact information.
  - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.
  - Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.
  - Is reviewed and approved by designated Data Owner.
- Distributes copies of the contingency plan to key contingency personnel (identified by name and/or role) and organizational elements.
- Coordinates contingency planning activities with incident handling activities.
- Reviews the contingency plan for the information system at least annually.
- Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
- Communicates contingency plan changes to key contingency personnel (identified by name and/or role) and organizational elements.
- Protects the contingency plan from unauthorized disclosure and modification.

CP-2 (1) Coordinate with Related Plans

Coordinates contingency plan development with organizational elements responsible for related plans.

CP-2 (3) Resume Essential Missions / Business Functions

Plans for the resumption of essential missions and business functions, within the time period agreed to by the Information System Owner and Data Custodian, when the contingency plan is activated.

CP-2 (8) Identify Critical Assets

Identifies critical information system assets supporting essential missions and business functions.

- Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations.
- The identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Organizational program protection plans can provide assistance in identifying critical assets.
    - Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms.
    - Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures).

CP-3 Contingency Training

MEDC IT, along with the system and/or data owner where applicable, will ensure that the following baseline controls are implemented and documented:

- Provides contingency training to information system users consistent with assigned roles and responsibilities:
    - Prior to assuming a contingency role or responsibility.
    - When required by information system changes.
    - Annually thereafter.

CP-4 Contingency Plan Testing

MEDC IT, along with the system and/or data owner where applicable, will ensure that the following baseline controls are implemented and documented:

- Tests the contingency plan for the information system at least annually using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan.
- Reviews the contingency plan test results.

- Initiates corrective actions, if needed.

CP-4 (1) Coordinate with Related Plans

Participates in contingency plan testing with organizational elements responsible for related plans.

CP-6 Alternate Storage Site

MEDC IT, along with the system and/or data owner where applicable, will ensure that the following baseline controls are implemented and documented:

- Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.
- Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

CP-6 (1) Separation from Primary Site

Identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

CP-6 (3) Accessibility

Identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-7 Alternate Processing Site

MEDC IT, along with the system and/or data owner where applicable, will ensure that the following baseline controls are implemented and documented:

- Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within a time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.
- Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption.
- Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

CP-7 (1) Separation from Primary Site

Identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

CP-7 (2) Accessibility

Identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7 (3) Priority of Service

Develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

CP-8 Telecommunications Services

MEDC IT, along with the system and/or data owner where applicable, will ensure that the following baseline controls are implemented and documented:

- Establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within one week of contingency plan activation when primary telecommunications capabilities are unavailable.

CP-8 (1) Priority of Service Provisions

- Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).
- Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8 (2) Single Points of Failure

Obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-9 Information System Backup

MEDC IT, along with the system and/or data owner where applicable, will ensure that the following baseline controls are implemented and documented:

- Conducts backups of system-level information contained in the information system at a frequency consistent with business unit recovery time and recovery point objectives.
    - System-level information includes, for example, system-state information, operating system and application software, and licenses.

- Conducts backups of user-level information contained in the information system at a frequency consistent with business unit recovery time and recovery point objectives.
  - User-level information includes any information other than system-level information.
- Conducts backups of information system documentation including security-related documentation at a frequency consistent with business unit recover time and recovery point objectives.
  - Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control.
- Protects the confidentiality, integrity, and availability of backup information at storage locations.

CP-9 (1) Testing for Reliability / Integrity

Tests backup information at least annually to verify media reliability and information integrity.

CP-10 Information System Recovery and Reconstitution

MEDC IT, along with the system and/or data owner where applicable, will ensure that the following baseline controls are implemented and documented:

- Provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

CP-10 (2) Transaction Recovery

The information system implements transaction recovery for systems that are transaction-based.

- Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

Compliance

National Institute of Standards and Technology (NIST) Special Publication 800-53A, Assessing Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf) from the NIST Computer Security Resource Center (http://csrc.nist.gov/publications/PubsSPs.html).

Authoritative Policies:	**SECU.01**
Associated Procedures:	**N/A**

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: 2018.10.01 13:27:33 -04'00'	September 19, 2018

Author:	Approver:	Approval Date:	Description of Change(s):
Terry Wood	Tilak Mohan	September 19, 2018	Original copy approval.

Issued Date:	Last Revision:	Last Reviewed:	Next Review Date:
September 19, 2018	September 19, 2018	September 19, 2018	September 19, 2019