MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	**MICHIGAN ECONOMIC DEVELOPMENT CORPORATION** Information Technology	**Standard:** **SECU.01.120.01**
Topic Area:	**Physical and Environmental Protection Standard**	
Distribution:	**All Michigan Economic Development Corporation Staff**	

Purpose:

To define the Physical and Environmental Protection 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, Physical and Environmental Protection (PE).

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 Physical and Environmental Protection. 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 Physical and Environmental Protection have been taken directly from NIST Special Publication 800-53 and have been modified in some cases for MEDC implementation.

This standard dictates the Physical and Environmental Protection security controls for every MEDC information system. These are identified as the MEDC minimum Physical and Environmental Protection 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 Information System (CJIS) security requirements) and should comply accordingly.

THE CONTROLS

PE-2 Physical Access Authorizations

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

- Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides.
- Issues authorization credentials for facility access.
- Reviews the access list detailing authorized facility access by individuals at least annually.
- Removes individuals from the facility access list when access is no longer required.

PE-3 Physical Access Control

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

- Enforces physical access authorizations at entry/exit points to the facility where the information system resides by:
    - Verifying individual access authorizations before granting access to the facility.
    - Controlling ingress/egress to the facility using physical access control systems/devices and guards.
- Maintains physical access audit logs for entry/exit points.
- Provides security safeguards to control access to areas within the facility officially designated as publicly accessible.
    - Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas.
- Escorts visitors and monitors visitor activity in all circumstances within restricted access area where the information system resides.
- Secures keys, combinations, and other physical access devices.

- Inventories physical access devices at least annually.
    - Physical access devices include, for example, keys, locks, combinations, and card readers.
    - Physical access control systems comply with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.
- Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

PE-4 Access Control for Transmission Medium

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

- Controls physical access to information system distribution and transmission lines within organizational facilities using security safeguards.
    - Security safeguards to control physical access to system distribution and transmission lines include, for example, locked wiring closets, disconnected or locked spare jacks and/or protection of cabling by conduit or cable trays.

PE-5 Access Control for Output Devices

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

- Controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
    - Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel.
    - Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

PE-6 Monitoring Physical Access

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

- Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.

  - Security incidents include, for example, apparent security violations or suspicious physical access activities.

- Reviews physical access logs upon occurrence of suspicious activity or persons.
  - Suspicious physical access activities include, for example, accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.
- Coordinates results of reviews and investigations with the MEDC incident response capability.

PE-6 (1) Intrusion Alarms / Surveillance Equipment

Monitors physical intrusion alarms and surveillance equipment.

PE-8 Visitor Access Records

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

- Maintains visitor access records to the facility where the information system resides for at least a year.
- Reviews visitor access records upon occurrence of suspicious activity or persons.
  - Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited.
  - Visitor access records are not required for publicly accessible areas.

PE-9 Power Equipment and Cabling

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

- Protects power equipment and power cabling for the information system from damage and destruction.
  - Protection includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

PE-10 Emergency Shutoff

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

- Provides the capability of shutting off power to the information system or individual system components in emergency situations.
- Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel.
- Protects emergency power shutoff capability from unauthorized activation.
    - This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

PE-11 Emergency Power

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

- Provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to long-term alternate power in the event of a primary power source loss.

PE-12 Emergency Lighting

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

- Employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
- This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

PE-13 Fire Protection

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

- Employs and maintains fire suppression and detection devices/systems for the information system that is supported by an independent energy source.
    - Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

PE-13 (3) Automatic Fire Suppression

Employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

PE-14 Temperature and Humidity Controls

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

- Maintains temperature and humidity levels within the facility where the information system resides at a level consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE), document entitled Thermal Guidelines for Data Processing Environments.
- Monitors temperature and humidity levels continuously.

PE-15 Water Damage Protection

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

- Protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
    - Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

PE-16 Delivery and Removal

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

- Authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items.
    - Effectively enforcing authorizations for entry and exit of information system components may require restricting access to

delivery areas and possibly isolating the areas from the information system and media libraries.

PE-17 Alternate Work Site

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

- Employs appropriate security controls at alternate work sites.
    - Alternate work sites may include, for example, government facilities or private residences of employees.
    - Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.
- Assesses as feasible, the effectiveness of security controls at alternate work sites.
- Provides a means for employees to communicate with information security personnel in case of security incidents or problems.
    - This control supports the contingency planning activities of organizations and the federal telework initiative.

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:	Not Applicable

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 13:37:01 -04'00'	September 27, 2018

Author:	Approver:	Approval Date:	Description of Change(s):
Kim Fedewa	Tilak Mohan	November 17, 2016	Original copy approval.
Kim Fedewa	Tilak Mohan	September 27, 2018	Removed Monthly tasks to upon occurrence of suspicious activity.