MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	**MICHIGAN ECONOMIC** **DEVELOPMENT CORPORATION** Information Technology	**Standard:** **SECU.01.180.01**
Topic Area:	**System and Information Integrity Standard**	
Distribution:	**All Michigan Economic Development Corporation Staff**	

Purpose:

To define the System and Information Integrity 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, System and Information Integrity (SI).

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 System and Information Integrity. 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 System and Information Integrity have been taken directly from NIST Special Publication 800-53 and have been modified in some cases for MEDC implementation.

This standard dictates the System and Information Integrity security controls for every MEDC information system. These are identified as the MEDC minimum System and Information Integrity 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

SI-2 Flaw Remediation

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

- Identifies, reports, and corrects information system flaws.
- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
- Installs security-relevant software and firmware updates in accordance with MEDC *SECU.01.150.01: Risk Assessment Standard*.
    - Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.
    - Time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw).
- Incorporates flaw remediation into the MEDC configuration management process.
    - Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow United States Computer Emergency Readiness Team (US-CERT) guidance and Information Assurance Vulnerability Alerts.
    - Some types of flaw remediation may require more testing than other types.
    - MEDC IT determines the degree and type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed.
        - In some situations, MEDC IT may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates.
        - MEDC IT may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

SI-2 (2) Automated Flaw Remediation Status

MEDC IT centrally manages the flaw remediation process and installs software updates automatically.

SI-3 Malicious Code 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 malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
    - Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices.
    - Malicious code includes, for example, viruses, worms, Trojan horses, and spyware.
    - Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.
- Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.
- Configures malicious code protection mechanisms to:
    - Perform scans of the information system continuously and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with the MEDC IT security policy.
    - Block and/or quarantine malicious code and send alerts to the administrator, Information System Owner and/or Data Custodian in response to malicious code detection.
- Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

SI-3 (1) Central Management

Centrally manages malicious code protection mechanisms.

- Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls.

SI-3 (2) Automatic Updates

The information system automatically updates malicious code protection mechanisms.

- Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, MEDC IT will give careful consideration to the methodology used to carry out automatic updates.

SI-4 Information System Monitoring

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

- Monitors the information system to detect:
    - Attacks and indicators of potential attacks in accordance with MEDC IT policies and procedures.
    - Unauthorized local, network, and remote connections.
        - Information system monitoring includes external and internal monitoring.
- Identifies unauthorized use of the information system through administrator log reviews.
- Deploys monitoring devices:
    - Strategically within the information system to collect organization-determined essential information.
    - At ad hoc locations within the system to track specific types of transactions of interest to the organization.
- Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
- Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal and state laws, executive orders, directives, policies, or regulations.
- Provide information system monitoring information to Information System Owners, Data Owners, and Data Custodians at least on a quarterly basis.

SI-4 (2) Automated Tools for Real-Time Analysis

Employs automated tools to support near real-time analysis of events.

- Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security

Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.

SI-4 (4) Inbound and Outbound Communications Traffic

The information system monitors inbound and outbound communications traffic on a continual basis, at the enterprise level, for unusual or unauthorized activities or conditions.

- Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems.
- Evidence of malicious code is used to identify potentially compromised information systems or information system components.

SI-4 (5) System-Generated Alerts

The information system alerts MEDC IT when the following indications of compromise or potential compromise occur:

- Presence of malicious code.
- Unauthorized export of information.
- Signaling to an external information system.
- Potential intrusions.

SI-5 Security Alerts, Advisories, and Directives

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

- Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.
- Generates internal security alerts, advisories, and directives as deemed necessary.
- Disseminates security alerts, advisories, and directives to appropriate personnel including, but not limited to, Admins, Information System Owners and Data Custodians.
- Implements security directives in accordance with established time frames or notifies the issuing organization of the degree of noncompliance.

SI-7 Software, Firmware, and Information Integrity

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

- Employs integrity verification tools to detect unauthorized changes to software, firmware, and information.
  - State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

SI-7 (1) Integrity Checks

The organization reassesses the integrity of software and information by performing daily integrity scans of the information system.

SI-7 (7) Integration of Detection and Response

Incorporates the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability.

- Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.

SI-8 Spam 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 spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
  - Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers.
- Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
  - Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses.
  - Spam protection mechanisms include, for example, signature definitions.

SI-8 (1) Central Management

Centrally manages spam protection mechanisms.

- Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls.

SI-8 (2) Automatic Updates

The information system automatically updates spam protection mechanisms.

SI-10 Information Input Validation

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

- The information system checks the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.
  - Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content.
  - Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components.
  - Structured messages can contain raw or unstructured data interspersed with metadata or control information.
  - If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata.
    - Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly.
  - Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands.
  - Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

SI-11 Error Handling

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

- The information system:
  - Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
  - Reveals error messages only to authorized personnel.

SI-12 Information Handling and Retention

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

- Handles and retains information within the information system and information output from the system in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, and operational requirements.

SI-16 Memory Protection

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

- The information system implements **security safeguards** to protect its memory from unauthorized code execution.
  - Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization.
  - Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

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 13:42:25 -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	April 4, 2017	Annual Review
Kim Fedewa	Tilak Mohan	September 27, 2018	Standardized verbiage for Scope, Purpose, and Standard. Replaced various DTMB organizations with appropriate MEDC teams.

Issued Date:	Last Revision:	Last Reviewed:	Next Review Date:
November 17, 2016	September 27, 2018	September 27, 2018	September 27, 2019