MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	**MICHIGAN ECONOMIC DEVELOPMENT CORPORATION** Information Technology	**Standard:** **SECU.01.170.01**
Topic Area:	**System and Communications Protection Standard**	
Distribution:	**All Michigan Economic Development Corporation Staff**	

Purpose:

To define the System and Communications 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, System and Communications Protection (SC).

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 Communications 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 System and Communications 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 System and Communications Protection security controls for every MEDC information system. These are identified as the MEDC minimum System and Communications 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

SC-2 Application Partitioning

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 separates user functionality (including user interface services) from information system management functionality.
    - Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.
    - The separation of user functionality from information system management functionality is either physical or logical.
    - Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate.
    - This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources.
    - Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

SC-4 Information in Shared Resources

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 prevents unauthorized and unintended information transfer via shared system resources.
    - This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources

(e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

- The control of information in shared resources is also commonly referred to as object reuse and residual information protection.
- This control does not address:
    - Information remanence which refers to residual representation of data that has been nominally erased or removed.
    - Covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions.
    - Components within information systems for which there are only single users/roles.

SC-5 Denial of Service 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 protects against or limits the effects of a Distributed Denial of Service attack (DDOS) by employing boundary protection devices and increased capacity and bandwidth combined with service redundancy.

SC-7 Boundary 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:
    - Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.
    - Implements subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks.
    - Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
        - Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

    - Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.
    - Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services.
    - Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

SC-7 (3) Access Points

Information System Owner and the Data Custodian will limit the number of external network connections to the information system.

SC-7 (4) External Telecommunications Services

- Implements a managed interface for each external telecommunication service.
- Establishes a traffic flow policy for each managed interface.
- Protects the confidentiality and integrity of the information being transmitted across each interface.
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need.
- Reviews exceptions to the traffic flow policy at least annually and removes exceptions that are no longer supported by an explicit mission/business need.

SC-7 (5) Deny by Default/Allow by Exception

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

- This control enhancement applies to both inbound and outbound network communications traffic.
- A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

SC-7 (7) Prevent Split Tunneling for Remote Devices

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

- This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, (e.g., notebook computers) and by prohibiting the connection if the remote device is using split tunneling.
- Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information.
- The use of virtual private networks (VPN) for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective.
    - VPNs thus provide a means for allowing non-remote communications paths from remote devices.
    - The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

SC-8 Transmission Confidentiality and Integrity

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 protects the confidentiality and integrity of transmitted information.
    - This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).
    - Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques).

SC-8 (1) Cryptographic or Alternate Physical Protection

The information system implements cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical safeguards.

- Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.
- Alternative physical security safeguards include, for example, protected distribution systems.

SC-10 Network Disconnect

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 terminates the network connection associated with a communications session at the end of the session or:
    - Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days.
    - Forcibly disconnects inactive Virtual Private Network (VPN) connections after fifteen (15) minutes of inactivity.

SC-12 Cryptographic Key Establishment and Management

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

- Establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with the hardware security module or other centralized format.
    - Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures.

SC-13 Cryptographic 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 the following Encryption Algorithms in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, and MEDC *SECU.01.170.03 Electronic Data Encryption Standard.*
    - Encryption Algorithms:
        - Asymmetric Keys:
            - Keys: RSA or DSA.
            - Size: 2048bit through 4096bit.

- Symmetric Keys:
  - Keys: AES or TDEA (3DES).
  - Size: Minimum 128bit, 192bit for low to moderate data.
  - 256bit for highly sensitive data.
- Hash Algorithm:
  - SHA-2 which include SHA-224 through SHA-512.
  - Session Encryption:
  - Transport Layer Security (TLS) version 1.1 or higher.
- Secure Shell (SSH):
  - Protocol 2 or later.

- This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: National Security Agency (NSA)-approved cryptography; provision of digital signatures: Federal Information Processing Standards (FIPS)-validated cryptography).

SC-15 Collaborative Computing Devices

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 prohibits remote activation of collaborative computing devices with the following exception: explicit authorization, in writing, by the CIO or designated representative.
  - Within this written authorization it is specifically identified the approved mechanisms, purpose and the information system upon which the mechanisms can be used.
  - No less than two factor authentication must be employed.
    - Collaborative computing devices include, for example, networked white boards, cameras, and microphones.
- The information system provides an explicit indication of use to users physically present at the devices.
  - Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

SC-17 Public Key Infrastructure Certificates

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

- Issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider.
    - For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores.
    - This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services.

SC-18 Mobile Code

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

- Defines acceptable and unacceptable mobile code and mobile code technologies.
    - Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.
    - Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.
- Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.
    - Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.
    - Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones).
- Authorizes, monitors, and controls the use of mobile code within the information system.

SC-19 Voice Over Internet Protocol

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

- Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.
- Authorizes, monitors, and controls the use of VoIP within the information system.

SC-20 Secure Name / Address Resolution Service (Authoritative Source)

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:
  - Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
  - Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
    - This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.
    - Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.
    - Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys.
    - DNS resource records are examples of authoritative data.
    - The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS.
    - The DNS security controls reflect (and are referenced from) The White House, Office of Management and Budget (OMB) Memorandum 08-23.
    - Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.

SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

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 requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
  - Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers.
  - Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.
  - DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.
  - Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.

SC-22 Architecture and Provisioning for Name / Address Resolution Service

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 systems that collectively provide name/address resolution service for the MEDC are fault-tolerant and implement internal/external role separation.
  - Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.
  - To eliminate single points of failure and to enhance redundancy, the MEDC employs at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server.
  - Additionally, MEDC typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility).

  - For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients).
  - DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet).
  - Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).

SC-23 Session Authenticity

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 protects the authenticity of communications sessions.
  - This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.
  - Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

SC-28 Protection of Information at Rest

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 protects the confidentiality and integrity of information at rest.
  - This control addresses the confidentiality and integrity of information at rest and covers user information and system information.
  - Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

SC-39 Process Isolation

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 maintains a separate execution domain for each executing process.
    - Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space.
    - Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.
    - Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces.
    - This capability is available in most commercial operating systems that employ multi-state processor technologies

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 13:41:08 -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	Standardized verbiage for Scope, Purpose, Standard. Added Compliance section.