MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	**MICHIGAN ECONOMIC DEVELOPMENT CORPORATION** **Information Technology**	**Standard:** **SECU.01.080.01**
Topic Area:	**Identification and Authentication Standard**	
Distribution:	**All Michigan Economic Development Corporation Staff**	

Purpose: To define the Identification and Authentication 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, Identification and Authentication (IA).

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

This standard dictates the Identification and Authentication security controls for every MEDC information system. These are identified as the MEDC minimum Identification and Authentication 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

IA-2 Identification and Authentication (Organizational Users)

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 uniquely identifies and authenticates system users (or processes acting on behalf of system users).
    - MEDC users include MEDC employees or individuals the MEDC has approved to handle MEDC data, for example, contractors and guests. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the MEDC in *SECU.01.020.01: Access Control Standard (AC-14)*. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.
    - Access to MEDC information systems is defined as either local or network.
        - Local access is any access to an MEDC information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network.
        - Network access is any access to an MEDC information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection.
            - Remote access is a type of network access which involves communication through an external or internal network (e.g., the Internet or local area network).
    - Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of MEDC.
    - For a virtual private network (VPN), the VPN is considered an internal network if the MEDC establishes the VPN connection between MEDC-controlled endpoints in a manner that does not require the MEDC to depend on any external networks across which the VPN traverses to protect the confidentiality and integrity of information transmitted.
    - Identification and authentication requirements for information system access by non-MEDC users are described in IA-8. In addition to identifying and authenticating users at the information system level, that is, at logon, identification and authentication

mechanisms are employed at the application level, when necessary, to provide increased information security for the MEDC.

IA-2 (11) Remote Access - Separate Device

The information system is capable of using multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- This reduces the likelihood of compromising authentication credentials stored on the system.
  - For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users.

IA-2 (12) Acceptance Of PIV Credentials

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

- Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to Federal Information Processing Standards (FIPS) Publication 201 and supporting guidance documents. The White House, Office of Management and Budget, OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable MEDC use of PIV credentials.

IA-3 Device Identification and Authentication

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 uniquely identifies and authenticates devices before establishing a network connection.
  - Organizational devices requiring unique device-to-device identification and authentication may be defined by type, device, or a combination of the two.
  - Information systems typically use either shared known information (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or business unit authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or the wide area network.

  - The MEDC Data Center Team determine the required strength of authentication mechanisms by the security categories of information systems.

IA-4 Identifier Management

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

- Manages information system identifiers by:
  - Receiving authorization from the designated business unit to assign an individual, group, role, or device identifier.
  - Selecting an identifier that identifies an individual, group, role, or device.
  - Assigning the identifier to the intended individual, group, role, or device.
  - Preventing the reuse of identifiers until all previous access authorizations are removed from the system, including all file access for that identifier, and not before a period of at least 365 days has passed.
  - Disabling the identifier after **90 days of inactivity.**
    - Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers.
    - Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts).
    - Generally, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4.
    - This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems).
    - Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

IA-5 Authenticator Management

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

- Manages information system authenticators by:
  - Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
  - Establishing initial authenticator content defined by the organization.
  - Ensuring that authenticators have sufficient strength of mechanism for their intended use.
  - Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
  - Changing default content of authenticators prior to information system installation.
  - Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.
  - Changing/refreshing authenticators:
    - Users no longer than every 90 days.
    - Privileged Users no longer than 90 days.
    - Personal Identity Verification (PIV)-compliant access cards are valid for no longer than 5 years.
    - Public Key Infrastructure (PKI) certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than 3 years.
  - Protecting authenticator content from unauthorized disclosure and modification.
  - Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators.
  - Changing authenticators for group/role accounts when membership to those accounts changes.
    - Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (i.e., the initial password) as opposed to requirements about authenticator content (i.e., minimum password length).
    - In many cases, developers ship information system components with factory default authentication credentials to allow for

initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and can present a significant security risk.

- The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges).
- Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication.
- Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately.
- Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance.
- Device authenticators include, for example, certificates and passwords.

IA-5 (1) Password-Based Authentication

The information system, for password-based authentication:

- Enforces minimum password complexity consisting of:
  - Contains at least eight characters.
  - Contains characters from three of the following four categories:
    - Uppercase alphabet characters (A–Z).
    - Lowercase alphabet characters (a–z).
    - Arabic numerals (0–9).
    - Non alphanumeric characters (for example,!$#,%).
  - Refer to *SECU.01.080.02 Active Directory Password Standard* for password types and complexity information.

- Enforces at least the following number of changed characters when new passwords are created: 1.
  - The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password.
- Stores and transmits only cryptographically-protected passwords.
- Enforces password minimum and maximum lifetime restrictions of one day minimum and 90 day maximum for user accounts.
  - Password lifetime restrictions do not apply to temporary passwords.
- Prohibits password reuse for at least 24 generations.
- Allows the use of a temporary password for system logons with an immediate change to a permanent password.
  - This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators.
  - To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.
- The Infrastructure Services, Director, must approve exceptions to password based authentication requirements.
  - Requests for exceptions should be sent to the MEDC IT Helpdesk.
  - Approved and denied exceptions will be documented.
  - A list of approvals and denials will be maintained showing:
    - User name, account, type of exception requested, approval or denial, date of request, date of approval / denial, type of exception.
    - Types of exceptions to be considered: Password changes every 180 days to password can never change; Owner can change password to owner cannot change password;

IA-5 (2) PKI-Based Authentication

The information system, for PKI-based authentication:

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
- Enforces authorized access to the corresponding private key.
- Maps the authenticated identity to the account of the individual or group.

- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
  - Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses.
  - For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing.

IA-5 (3) In-Person Or Trusted Third-Party Registration

Requires that the registration process to receive all hardware/biometric (multifactor authenticators) be conducted in person before a designated registration authority with authorization by an Authorizing Official.

IA-5 (11) Hardware Token-Based Authentication

The information system, for hardware token-based authentication, employs mechanisms that satisfy token quality requirements as defined by the Data Center Team.

- Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the United States (U.S.) Government Personal Identity Verification (PIV) card.
- Organizations define specific requirements for tokens, such as working with a particular PKI.

IA-6 Authenticator Feedback

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 obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
  - The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms.
  - Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

IA-7 Cryptographic Module Authentication

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 mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal and state laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

IA-8 Identification and Authentication (Non-Organizational Users)

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 uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
    - Non-organizational users include information system users other than organizational users explicitly covered by IA-2 in this standard. Non-organizational users are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14.
    - In accordance with the *E-Authentication E-Government* initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems).
    - Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk.

IA-8 (1) Acceptance of PIV Credentials From Other Business Units

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other MEDC business units.

- This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS).
- Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable MEDC use of PIV credentials.

IA-8 (2) Acceptance of Third-Party Credentials

The information system accepts only Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials.

- This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites.
- Third-party credentials are those credentials issued by nonfederal government entities approved by the FICAM Trust Framework Solutions initiative.
    - Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.

IA-8 (3) Use of FICAM-Approved Products

Employs only FICAM-approved information system components in information systems to accept third-party credentials.

- This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites.
- FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program.

IA-8 (4) Use of FICAM-Issued Profiles

The information system conforms to FICAM-issued profiles.

- Addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements.
- The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange).

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 13:28:12 -04'00'	September 19, 2018

Author:	**Approver:**	**Approval Date:**	**Description of Change(s):**
Kim Fedewa	Tilak Mohan	November 17, 2016	Original copy of approval.
Kim Fedewa	Tilak Mohan	April 3, 2017	PW Length = 14, Change PW every 180 days, cannot reuse last 24 passwords.
Kim Fedewa	Tilak Mohan	July 6, 2017	PW Length = 8, Change PW every 90 days. Removed IA-2(1) thru IA-2 (8) ~ multifactor requirement for using administrative accounts. Created Password Exception List requirements - IA-5 (1).
Kim Fedewa	Tilak Mohan	September 19, 2018	Revised much verbiage to comply with NIST and DTMB.