| MICHIGAN ECONOMIC DEVELOPMENT CORPORATION | **MICHIGAN ECONOMIC DEVELOPMENT CORPORATION**<br>Information Technology | **Standard:**<br>**SECU.01.020.01** |
|---|---|---|
| **Topic Area:** | **Access Control Standard** | |
| **Distribution:** | **All Michigan Economic Development Corporation Staff** | |

**Purpose:**

To define the Access Control 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, Access Control (AC).

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

This standard dictates the Access Control security controls for every MEDC information system. These are identified as the MEDC minimum Access Control 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

### AC-2 Account Management

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

- Information systems account types are identified.
- Account Managers are assigned.
- Conditions for group and role membership are established.
- Authorized users, role membership, and authorized access for each account are specified.
    - Requires approvals by System Owner and/or other appropriate personnel for requests to create information system accounts.
    - Creates, enables, modifies, disables, and removes information system accounts in accordance with MEDC approved policies, standards, and procedures that are NIST compliant.
    - Monitors the use of information system accounts.
- Business units must notify Data Owners when accounts are no longer required, when users are terminated or transferred, and when individual information system usage privileges change.
- Access to information systems is based on valid access authorization, intended system usage and other attributes defined by the System Owner.
- Data Owners can define access privilege or other attributes by account, by type or combination, and may include dynamic privilege management but must include restrictions on the time of day, day of week, and point of origin. A level of confidence and authentication for each user must be established. Administrative privileges receive additional scrutiny.
- Accounts are recertified for compliance with standard account management requirements. The account recertification process includes the following:
    - Performed annually
    - Validate all accounts are needed
    - Validate each account has an owner
    - Validate data permissions assigned to each account are based on the principle of least privilege
    - Initiate a removal / disable process for unneeded accounts.

- A procedure is established to reissue shared/group credentials (if deployed) when individuals are removed from a group.

**AC-2 (1) Automated System Account Management**

- Employ automated mechanisms to support the management of information system accounts.
    - Automated mechanisms can include using the information system, email, text messaging, or telephonic communication to automatically monitor account usage, including termination or transfer of user accounts and atypical system account usage.

**AC-2 (2) Removal of Temporary/Emergency Accounts**

Temporary/Emergency accounts are manually deleted or disabled when access is no longer needed.

**AC-2 (3) Disable Inactive Accounts**

The information system tracks inactive user system accounts. Data Owners and MEDC IT review inactive accounts monthly and disable, remove or leave as is. Inactive accounts are defined as accounts that show no activity for 60 days.

**AC-2 (4) Automated Audit Actions**

The information system automatically audits account creation, modification, disabling, and removal actions and notifies, as required, appropriate individuals such as MEDC IT or System Owners.

**AC-3 Access Enforcement**

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

- Information systems enforce authorizations as approved by MEDC IT for logical access to the system resources in accordance with applicable access control policies.
    - Control policies that are utilized can be mandatory policies, discretionary and identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms, such as access control lists, access control matrices and cryptography can be used to control access between users (or processes acting on behalf of users) and objects, such as devices, files, data, processes, programs or domains within the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the MEDC.

**AC-4 Information Flow Enforcement**

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 enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on the use of Enterprise Network Security Devices as outlined in MEDC *INFRA.01.009 Firewall and MEDC-NET Perimeter Security Standard.*

**AC-5 Separation of Duties**

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

- Separation of duties of individuals must be implemented through assigned information system access authorizations. Access authorizations defined in this control are implemented by the Access Enforcement Control (AC-3).
    - Duties should be separated: when mission functions and distinct information system support functions are divided among different individuals/roles; if different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); when the security personnel who administer access control functions do not administer audit functions; and if there are different administrator accounts for different roles.

**AC-6 Least Privilege**

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

- Least privilege permits only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with roles and responsibilities of job functions.
    - The MEDC employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to MEDC operations and assets, and individuals.

**AC-6 (1) Authorize Access to Security Functions**

Identify authorized personnel (security administrators, system and network administrators, system programmers, and other privileged users) and define security functions, such as establishing system accounts, configuring access authorizations (i.e., permissions, privileges) setting events to be audited, and setting intrusion detection parameters.

**AC-6 (2) Non-privileged Access for Non-Security Functions**

Define the security functions or sensitive information and require that users of information system accounts, or roles, with access to this information use non-privileged accounts, or roles, when accessing non-security system functions.

**AC-6 (5) Privileged Accounts**

Limit authorization to privileged accounts on the information system to roles designated by the System Owner.

- The MEDC may differentiate in the application of this control between allowed privileges for local information system accounts and for domain accounts provided the MEDC retains the ability to control the configuration of the system with regard to key security parameters and as otherwise necessary to sufficiently mitigate risk.

**AC-6 (9) Auditing of Privileged Functions**

The information system audits the execution of privileged functions, thus detecting misuse, and in doing so, helps mitigate the risk from insider threats and the advanced persistent threat (APT).

**AC-6 (10) Prohibit Non-Privileged Users from Executing Privileged Functions**

The information system prevents non-privileged users from executing privileged functions. This includes disabling, circumventing, or altering implemented security safeguards/countermeasures.

**AC-7 Unsuccessful Logon Attempts**

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 enforces a limit of three invalid logon attempts within a fifteen-minute time period during a user session upon which the account/node is automatically locked for a minimum period of 30 minutes or until released by an administrator.
    - Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically released after a predetermined time period established

by the MEDC. This control applies to all accesses other than those accesses explicitly identified and documented by the MEDC.

**AC-8 System Use Notification**

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 displays an approved system use notification message or warning banner before granting access to the system. This message provides privacy and security notices consistent with applicable state and/or federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. It states that users are accessing MEDC information system; that usage may be monitored, recorded, and subject to audit; that unauthorized use of the system is prohibited; and that use of the system indicates consent to monitoring and recording.
- The notification message or banner remains on the screen until users take explicit actions to log on or further access the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.
- For publicly accessible systems, the information system displays the system use information before granting further access; displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and includes a description of the authorized uses of the system.

**AC-11 Session Lock**

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 further access to the system by initiating a session lock after 10 minutes of inactivity of an operating system, after 15 minutes of inactivity for applications or upon receiving a request from a user and retains the session lock until the user re-establishes access using established identification and authentication procedures.

**AC-11 (1) Pattern-Hiding Displays**

The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern (an image

that does not convey sensitive information) onto the associated display, concealing what was previously visible on the screen.

**AC-12 Session Termination**

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

- Define conditions and trigger events requiring automatic session termination of user applications and ensure that the information system enforces these parameters.
- A logical session is initiated whenever a user accesses the information system and can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the System Owner to continue after the session is terminated. Conditions or trigger events can include, for example, business units-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions.

**AC-14 Permitted Actions Without Identification or Authorization**

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

- Identify specific user actions that can be performed on the information system without identification or authentication.
- Document and provide supporting rationale for the information system concerning user actions not requiring identification and authentication.
- It is not, however, mandating that such instances exist in a given information system. The System Owner must permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives. MEDC business units may deem necessary an emergency bypass be used, for example, via a software-readable physical switch that commands bypass of the login functionality and is protected from accidental or unmonitored use.

**AC-17 Remote Access**

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

- Establish and document usage restrictions and implementation guidance for each allowed remote access control.
- Machine to machine communication must be authenticated prior to sending data and must be encrypted. Authentication mechanisms must be through mutual certificate exchange, public key authentication, or

symmetric key exchange along with the ability to white list source Internet Protocol (IP) addresses.

- All system-owners must employ a two-factor authentication to direct access information system resources located in a trusted MEDC Zone from and un-trusted network (i.e., the Internet).
- Authorize remote access prior to connection. This authorization format is not specified. For example, while the MEDC may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control.
    - Remote access is any access to a MEDC information system by a user (or process acting on behalf of a user) communicating through an external network such as the Internet.
    - Remote administration to an IT resource from an untrusted network must be accomplished through the use of a virtual private network VPN connection.
    - A VPN, when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the State of Michigan (SOM) establishes a network connection between SOM-controlled endpoints and MEDC endpoints in a manner that does not require the SOM to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls do not apply to public web servers or systems specifically designed for public access.
- Identified and approved methods for remote vendor access are as follows:
    - Secure ID through VPN-Vendor is provided with a Secure ID token and VPN software in order to access MEDC resources.
- MEDC IT resources, which are accessed by a remote vendor, must have security logging configured and enabled by their System Administrator. In addition, the System Administrator must review the logs in accordance with the regulatory requirements for which the asset is in scope (e.g., Internal revenue Service (IRS) Publication 1075, Payment Card Industry Data Security Standard (PCI-DSS), Criminal Justice Information System Policy (CJIS), etc.). IT Resources not in scope for regulatory requirements will be reviewed every 30 days. All suspected security incidents must be reported using MEDC *SECU.01.090.01.01: How to Handle a Security Breach Procedure.*
- Under contract with MEDC, vendors must adhere to current SOM and MEDC policies and standards.

**AC-17 (1) Automated Monitoring/Control**

Automated mechanisms to facilitate the monitoring and control must be employed. Automated monitoring of remote access sessions allows the MEDC to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with the remote access policy.

**AC-17 (2) Protection of Confidentiality/Integrity Using Encryption**

The information system implements a cryptography mechanism to protect the confidentiality and integrity of remote access session. The encryption strength of mechanism is selected based on the security categorization of the information. Refer to MEDC *SECU.01.170.03: Electronic Data Encryption Standard.*

**AC-17 (3) Managed Access Control Points**

The information system routes all remote accesses through a limited number of managed network access control points.

- In an effort to reduce the attack surface for the MEDC, MEDC IT should determine a limited number of managed network access control points through which the information system routes remote access.

**AC-17 (4) Privileged Commands/Access**

Authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.

- Document the rationale for such access in the security plan for the information system.

**AC-18 Wireless Access**

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

- Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
    - Individuals and/or MEDC business units shall not implement their own network infrastructure. Only MEDC Infrastructure Services can set up business related wireless networks to ensure secure configuration, proper deployment, and standards of compliance.
- Authorize wireless access to the information system prior to allowing such connections.
    - Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

**AC-18 (1) Authentication and Encryption**

The information system protects wireless access to the system using authentication of users, devices or both as necessary and encryption.

**AC-19 Access Control for Mobile Devices**

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, configuration requirements, connection requirements, and implementation guidance for mobile devices.
    - Usage restrictions and implementation guidance to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possible other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared).
    - Mobile devices include portable storage media (e.g., Universal Serial Bus (USB) memory sticks, external hard drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). MEDC-controlled mobile devices include those devices for which the MEDC has the authority to specify and the ability to enforce specific security requirements.
- The connection of mobile devices to MEDC information systems is authorized.
- Monitor for unauthorized connections of mobile devices to MEDC information systems and enforce requirements for connections.
    - Information system functionality that provides the capability for automatic execution of code on mobile devices without user direction must be disabled. Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.
- Storage of sensitive information on MEDC-owned mobile devices or portable media is granted to individuals for a finite duration as needed to fulfill the specific functions required to perform a specific job. Approval must be obtained by either the employee's Supervisor or the system/data owner.

- When users are traveling to locations that the MEDC considers is a significant risk in accordance with system owner policies and procedures, specially configured mobile devices must be issued. MEDC IT must inspect and take preventative measures to these mobile devices upon return. MEDC policies and procedures for mobile devices used by individuals departing on and returning from travel include, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive.

**AC-19 (5) Full Device/Container-Based Encryption**

Employs full-device encryption for MEDC laptops and container encryption for hand-held mobile devices such as phones to protect the confidentiality and integrity of information on state-owned mobile devices.

- Storage of sensitive information is permitted only when sensitive data has been encrypted. Encryption must comply with MEDC *SECU.00.170.03: Electronic Data Encryption Standard* as published. Unencrypted storage of sensitive information on MEDC-owned mobile devices and portable media is prohibited. *MEDC SECU.01.110.04: Secure Disposal of Installed and Removable Digital Media* standard for data sanitation and media disposal will need to be followed.
- **Any** instance of MEDC sensitive information (including that stored on a mobile device or portable media-encrypted or unencrypted) being lost, stolen, or where there is reasonable belief that an unauthorized person may have acquired the data, must be reported immediately. Refer to MEDC *SECU.01.090.01.01: How to Handle a Security Breach* procedure.
- Any employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment and/or criminal prosecution where the act constitutes a violation of law. Any third party found to have violated this standard may be subject to action, up to and including criminal prosecution where the act constitutes a violation of law. A breach of contract and fiduciary liability may also apply.

**AC-20 Use of External Information Systems**

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

- Establishes terms and conditions, consistent with any trust relationships established with other system owners owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems, and process, store, and/or transmit system owner-controlled information using the external information systems.
- The terms and conditions shall address, at a minimum:
    - The types of applications that can be accessed on the MEDC information system from the external information system.
    - The Federal Information Processing Standards (FIPS) 199 security category of information that can be processed, stored, and transmitted on the external information system.
    - How other users of the external information system will be prevented from accessing MEDC information.
    - The use of VPN and firewall technologies.
    - The use of and protection against the vulnerabilities of wireless technologies.
    - The maintenance of adequate physical security controls.
    - The use of virus and spyware protection software.
    - How often the security capabilities of installed software are to be updated.
- External information systems include, but are not limited to: personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants), privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports), and MEDC information systems that are not owned by, operated by, or under the direct supervision and authority of the MEDC.
- For some external systems, in particular those systems operated by other states or the state agencies including agencies subordinate to those states, the trust relationships that have been established between those states and the originating state may be such, that no explicit terms and conditions are required. In effect, the information systems of these states would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or states subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies.
- Authorized individuals include MEDC personnel, contractors, or any other individuals with authorized access to the MEDC information

system and over which the MEDC has the authority to impose rules of behavior with regard to system access. The restrictions that the MEDC imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between states. The MEDC might impose more stringent security restrictions on a contractor than on a state, local, or tribal government. This control does not apply to the use of external information systems to access public interfaces to MEDC information systems and information.

**AC-20 (1) Limits on Authorized Use**

Permits authorized individuals to use an external information system to access the information system or to process, store, or transmit system owner-controlled information only when the system owner:

- Verifies the implementation of required security controls on the external system as specified in the system owner's information security policy; or verifies that the required security controls that have been implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the confidence level required by the MEDC IT.
- Retains approved information system connection or processing agreements with the system owner entity hosting the external information system.

**AC-20 (2) Portable Storage Devices**

Limits the use of portable storage devices by authorized individuals on external information systems. This may include prohibition or restrictions on how the devices may be used and under what conditions the devices may be used.

**AC-21 Information Sharing**

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

- Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information being shared.
- Employs automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.
    - Depending on the information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, or security category.

**AC-22 Publicly Accessible Content**

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

- Designate individuals authorized to post information onto a system owner information system that is publicly accessible.
- Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
    - Nonpublic information is any information for which the general public is not authorized access in accordance with MEDC and/or federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on a MEDC information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-MEDC information systems is covered by MEDC *SECU.01: Information Technology Information Security Policy.*
- Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.
- Review the content on the publicly accessible system quarterly, ensuring the public information is secure and removing nonpublic information if discovered.

**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<br>Digitally signed by Tilak Mohan<br>DN: cn=Tilak Mohan, o=Michigan Economic Development Corporation, ou=Information Services, email=mohant1@michigan.org, c=US<br>Date: 2018.10.01 13:22:53 -04'00' | September 18, 2018 |

| Author: | Approver: | Approval Date: | Description of Change(s): |
|---|---|---|---|
| Kim Fedewa | Tilak Mohan | November 17, 2016 | Original copy approval. |
| Kim Fedewa | Tilak Mohan | March 27, 2017 | Remove NIST mention in Purpose. Remove Supersedes language in Scope. Define Inactive account in AC-2(3). Incorporate CTRL.01.02 into AC-17 Remote Access section. |
| Kim Fedewa | Tilak Mohan | July 24, 2018 | Many grammatical / indentation errors fixed. |
| Kim Fedewa | Tilak Mohan | September 18, 2018 | Added recertification definition in step AC-2 Account Management. |